The Defense Science Board
1999 Summer Study Task Force

on

21ST CENTURY DEFENSE TECHNOLOGY STRATEGIES

Volume II
SUPPORTING REPORTS

March 2000

Office of the Under Secretary of Defense
For Acquisition & Technology
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

THIS REPORT IS UNCLASSIFIED. DISTRIBUTION IS UNLIMITED.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
March 2000

3. REPORT TYPE AND DATES COVERED
Final Technical, 2000

4. TITLE AND SUBTITLE
Report of the Defense Science Board Task Force on 21st Century Defense Technology Strategies, VOL II, Supporting Reports

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
Mr. Donald Latham and Dr. V. Larry Lynn, Co-chairs

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense
Pentagon, Rm. 3D865
Washington, DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense
Pentagon, Rm. 3D865
Washington, DC 20301-3140

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES
N/A

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release. Unlimited distribution.

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
322

16. PRICE CODE
N/A

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
UNCLASSIFIED	UNCLASSIFIED	N/A	N/A

TABLE OF CONTENTS

Preceding PageS Blank

PART I. INTELLIGENCE NEEDS AND ADVERSARIES

TERMS OF REFERENCE

"This task force will focus on the global national intelligence system needed to provide the United States and its allies adequate warning, with specifics, of developing military and technology capabilities which could threaten national security. The focus should include improved intelligence on development of nuclear, chemical, and biological weapons, their means of delivery, and associated adversary intelligence, command, control, and communications systems. Of particular concern is the potential rapid evolution of a major regional power and our intelligence capability to early and accurately detect evolving adversary capabilities and intent. The task force will take a "Red Team" view and consider how various potential adversaries might choose to invest in asymmetric capabilities which could threaten U.S. full spectrum conflict dominance over the next two decades. Detection of adversary developments which could threaten U.S. asymmetrical strengths (such as stealth, GPS, ISR, ASW, etc.) or take advantage of asymmetrical weaknesses (such as information system vulnerability, casualty aversion, etc.) is of high importance. Recommendations will be made for improving current systems and approaches."

EXECUTIVE SUMMARY

Collection and analysis of foreign intelligence is, and will continue to be, a vital component of U.S. national security strategy. However, there is significant debate regarding whether our existing intelligence apparatus can sufficiently transform itself to meet the demands of the 21st century. The Department of Defense (DoD) has a vested interest in this debate – both as a customer and as a major supplier – because the goals of the National Military Strategy cannot be achieved in the absence of a robust foreign intelligence apparatus.

This task force first examined the anticipated 21st century threat environment, focusing on how the threats and adversaries are changing in the post-Cold War era. We then worked to characterize future intelligence customers' needs, again emphasizing how the dynamic global security environment is altering both needs and expectations. Finally, we formulated a top-level opinion of the strategic posture of today's Intelligence Community (IC) and its ability to meet the needs of its primary DoD customers – with particular emphasis on the warfighter. Our recommendations are intended to better position the IC to meet the evolving demands of its diverse customer base.

The global technology environment – fueled by the explosion in information technologies – provides the strategic context for our report. The most dramatic changes have occurred within the past decade – that is, since the end of the Cold War. These changes are enhancing our adversaries' abilities to threaten our nation's interests – simultaneously expanding both the needs and expectations of intelligence customers – and are confronting the IC with both challenges and opportunities to dramatically improve its performance.

Few would question our military dominance as we enter the 21st century. It is increasingly likely that future adversaries will choose to avoid head-to-head conflict as a result, preferring instead to exploit asymmetric options. It is equally clear that our adversaries know a great deal about our legacy capabilities and are using this knowledge to deny and to deceive our intelligence apparatus. But it remains true that any adversary intending harm to U.S. national interests will do so in secret. In fact, the greater the asymmetric advantage perceived by the adversary, the more energetic will be the denial and deception. This situation demands that our intelligence apparatus identify, detect and analyze the new observables that will provide the necessary insights into the actions and intentions of our adversaries.

The emerging challenge is exacerbated by the fact that many of our potential adversaries are highly mobile, widely distributed, and technologically sophisticated. While our adversaries are less anchored to geography than in the past, our warfighters' need for precision intelligence – e.g. to guide their precision weapons – is growing. And our adversaries are getting smarter and more capable. The technology gap between our own capabilities and those of our adversaries is narrowing due to the expanding availability of sophisticated technologies. Information once confined to national programs is increasingly available in the commercial marketplace – potentially nullifying our presumption of information dominance. A successful 21st century intelligence apparatus will enable *decision superiority* – the step beyond information superiority.

The luxury of focusing on a relatively stable threat environment is gone forever – replaced by the expectation that our intelligence apparatus will support diverse policy issues and military operations spanning the spectrum from peacekeeping and humanitarian missions to warfighting and defending our homeland. At the same time, customers have access to a wealth of relevant information from other sources – and sometimes wish to perform their own interpretation and fusion of the available data. So the intelligence apparatus faces the dual challenge of providing key customers with more robust access to intelligence data – while at the same time assimilating the broader information domain into their own analytic insights and judgments.

It is clear that our intelligence apparatus must more effectively exploit technological advances in responding to these challenges. But it must proceed with caution, because indiscriminate use of commercial-off-the-shelf (COTS) technologies will introduce potentially serious vulnerabilities. The intelligence apparatus must effectively balance the need to protect its own information assets while still providing timely intelligence to its primary customers – whose information resources are equally vulnerable to attack.

We concluded that our existing intelligence apparatus is not currently well-postured, nor are robust strategies in place, to cope with current and emerging customer demands. Our recommendations range from better allocation of resources against critical intelligence missions to enabling greater agility in responding to dynamic priorities. The Defense Science Board's (DSB) goal is to create a 21st century Intelligence Enterprise that is:

- Robust against widely diverse issues – while maintaining sufficient depth on each issue to enable precision operations
- Agile amidst rapidly changing priorities – while maintaining vigilance over important strategic issues
- Anticipatory – able to forecast the important changes in global conditions
- Fully integrated with the customer communities it serves

We modeled our recommendations after the DoD structure and assignment of roles and responsibilities.

The DSB's first recommendation is intended to sharpen the focus and better align intelligence resource allocation with intelligence mission objectives. In today's IC, the resource allocation process is dominated by collectors, whose natural desire is to optimize the performance of their discipline-specific capabilities. We believe customers would be better served if Mission Managers, directly responsible for delivering intelligence to users, had a dominant voice in the resource allocation process.

Our second recommendation tackles the problem of fully integrating the activities of the intelligence apparatus – both among intelligence components and together with its primary customers. We address three dimensions that we believe are critical performance enablers:

- Security policy
- Information infrastructure
- Operational processes

We focus specifically on two core processes – collaboration and TPED (tasking, processing, exploitation, and dissemination) – emphasizing the need for integration with DoD and other customers in both.

Our third recommendation targets the challenge of continuous transformation – the ongoing infusion of new capabilities into our intelligence apparatus to meet the demands of an ever-changing threat environment. We emphasize an end-to-end systems approach, with particular focus on important problems explicitly derived from mission needs.

Finally, we recommend the development of strategies to sustain enterprise investment in critical skills and technologies. The long-term success of any information-based organization is dependent upon its intellectual assets. Given that every report and evaluation of the IC in recent years – including this study – has identified significant deficiencies in this area, we believe that strategic investment is imperative. We further recommend adoption of the "grand challenge" approach to focus technology investments – ensuring that individual projects are well-coordinated with DoD investments, but that the challenges are defined in terms of benefits to intelligence missions.

Our four major recommendations were crafted to build from one to the next rather than defining a set of independent actions. This is not to suggest that each recommendation in isolation is without value, but rather that the cumulative impact would be greater. We therefore end our report with a potential integrating framework. Our goal is to purposefully create a robust 21st century Intelligence Enterprise.

INTRODUCTION

"What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge."

Sun Tzu
On the Art of War

Effective intelligence is, and will continue to be, vital to maintaining our nation's security in the 21st century. There now appears to be little disagreement on this point, although many questions were voiced as we entered the post-Cold War era in the early 1990s. It also appears to be widely accepted that our existing intelligence apparatus is not well-equipped to deliver against the demands of the emerging national security environment. But that is the extent of the consensus. It is evident from the many articles, reports, and studies published during the past several years that there are numerous opinions, but no apparent agreement, on how best to satisfy our nation's need for effective intelligence. And there is significant debate regarding whether today's intelligence apparatus can sufficiently transform itself to meet the demands of the 21st century.

The efforts of this task force build from the previous studies and reports and propose a conceptual framework that would better enable our nation's intelligence apparatus to adapt itself to meet the emerging demands. We realize that many of the observations and recommendations are not new and gratefully acknowledge the contributions of previous authors. It is our belief, however, that the institutional response to these previous works is woefully inadequate when measured against the magnitude of change needed. We have therefore devoted considerable energy to understanding the impediments that currently inhibit change and have developed a set of recommendations that we believe will help overcome the major obstacles.

The task force recommendations span the spectrum from mission focus and functional integration issues to the need for continuous innovation and sustained investment. Because this study was tasked by the Defense Science Board, our first inclination was to identify areas in which technology-based solutions would enhance the intelligence mission performance. Our report contains some discussion along those lines, but we concluded early in our efforts that while more and better technology investments are necessary, they are by no means sufficient to position the intelligence apparatus to succeed against emerging threats and expanding customer demands. In fact, it seems that the organizational dynamics driving today's intelligence resource allocation processes are perhaps a larger problem than the adequacy of the resources being allocated.

THE INTELLIGENCE COMMUNITY

The collection of agencies and organizations that conduct the various intelligence activities that make up our national intelligence effort is referred to as the Intelligence Community. The IC crosses departmental and agency boundaries and is governed by multiple Executive Orders and statutes. The Director of Central Intelligence (DCI) serves simultaneously as the Director of the Central Intelligence Agency (CIA), the President's Intelligence Advisor, and the leader of the IC, of which the CIA is but one component.

IC membership includes components from five departments of the federal government and one independent agency. The various organizations serve an equally diverse customer set, ranging from the President, the Cabinet, and the Congress, at the national level, to deployed military forces at the tactical level. Components of the IC are listed below.[1]

Independent Agency
Central Intelligence Agency

Department of Defense
Defense Intelligence Agency (DIA)
National Security Agency (NSA)
National Imagery & Mapping Agency (NIMA)
National Reconnaissance Office (NRO)
Army Intelligence
Navy Intelligence
Air Force Intelligence
Marine Corps Intelligence

Department of State
Bureau of Intelligence & Research (INR)

Department of Energy
Foreign Intelligence Program

Department of Justice
Federal Bureau of Investigation (FBI)

Department of the Treasury
Office of Intelligence Support (OIS)

The DCI's role as leader of the IC is to oversee the *national* intelligence effort, which is comprised of the activities that support political, economic, and military decisionmakers. Resources for these activities make up the National Foreign Intelligence Program (NFIP), which is developed annually by the DCI under the authority of Executive Order 12333. The DCI is assisted in the planning and programming of resources by the Community Management Staff (CMS), which is headed by the Deputy Director of Central Intelligence for Community Management (DDCI for Community Management). NFIP resources comprise approximately 56 percent of the total intelligence budget.[2] Members of the IC advise the DCI through their participation on a number of committees established to address issues of common concern. Two of the primary committees are the National Foreign Intelligence Board (NFIB) and the Intelligence Community Executive Committee (IC EXCOM), which the DCI chairs.

The Intelligence Community Reform Act, part of the FY 1997 Intelligence Authorization Act, established the positions of Assistant Director of Central Intelligence (ADCI) for Collection and ADCI for Analysis and Production to assist the DCI and the DDCI for Community Management in carrying out their responsibilities. The ADCI for Collection is tasked to help ensure that the suite of collection assets is developed and operated in concert to provide efficient

[1] "U.S. Intelligence Community – Who We Are and What We Do." http://www.cia.gov/ic/functions.html

[2] Federation of American Scientists (FAS), Intelligence Resource Program, www.fas.org/irp/agency/budget2.htm

and effective collection of information. The ADCI for Analysis and Production is responsible for providing oversight of the IC analysis and production components, and is dual-hatted as the Chairman of the National Intelligence Council.

Intelligence activities that are more narrowly focused and intended to support the *tactical* needs of military forces are funded separately in two programs within the DoD. These programs, the Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA), fall under the purview of the Deputy Secretary of Defense and make up the remaining 44 percent of the total intelligence budget.[3] Given the blurring of the boundary between national and tactical intelligence objectives, the DCI and the Deputy Secretary of Defense have begun working to better align resource allocation processes across the NFIP, JMIP and TIARA programs. A key component of this process is the Intelligence Program Review Group (IPRG), which identifies, evaluates, and prioritizes crosscutting intelligence issues. This group provides recommendations to the Expanded Defense Resources Board (EDRB), which is co-chaired by the DCI and the Deputy Secretary of Defense.

Today's IC is the product of more than five decades of evolution of our national intelligence apparatus. The IC has been shaped by a series of statutes and Executive Orders that establish the governing legal authorities. Key documents include the National Security Act of 1947 (as amended), which established the basic organization of our national security effort, and Executive Order 12333, which provides guidelines for the conduct of intelligence activities and describes the composition of the IC. Major events in the history of the IC are shown in the following chart.

DoD Interests

The Department of Defense has a vested interest in the vitality of the intelligence apparatus – both as a primary customer and as a major supplier. Although not explicitly stated in Joint Vision 2010 (JV2010), it is evident that the vision of the Joint Chiefs of Staff (JCS) cannot be realized without the requisite intelligence.[4] Major themes emerging from the National Military Strategy – *Prepare for the Future, Shape the Environment, Respond to Contingencies*, and *Protect the Homeland* – are equally reliant on effective intelligence.[5] While the DoD does not "own" the IC, eight of the thirteen components are DoD organizations or agencies, and the DoD executes approximately 87 percent of the total budget for intelligence.[6] Three of the DoD components, National Security Agency (NSA), Defense Intelligence Agency (DIA), and National Imagery and Mapping Agency (NIMA), are designated as Combat Support Agencies, meaning that they provide tactical support to the warfighter in addition to their broader role in national intelligence. National Reconnaissance Organization (NRO), also a DoD component, supplies data collected via overhead assets to NSA and NIMA. The remaining four DoD components are service-specific and are chartered to meet the unique needs of their parent service.

[3] Ibid.

[4] "Joint Vision 2010," John M. Shalikashvili, Chairman of the Joint Chiefs of Staff.

[5] National Military Strategy.

[6] FAS, Intelligence Resource Program, www.fas.org/irp/agency/budget2.htm

In addition to components of the IC, there are a variety of other intelligence activities within the DoD that support joint operations. The ability of the joint force commanders to accomplish their objectives depends in part on efficient and effective cooperation – and contributions – from the entire suite of intelligence resources. The Joint Staff Directorate for Intelligence, J-2, directly supports the Chairman of the Joint Chiefs of Staff, the Office of the Secretary of Defense (OSD), the Joint Staff, and the combatant commands. The Joint Staff J-2 is a unique organization in that it is simultaneously a major component of the DIA and a fully integrated element of the Joint Staff. The Joint Staff J-2 operates the National Military Joint Intelligence Center (NMJIC), which serves as the national focal point for crisis intelligence in support of joint operations, and employs a national intelligence support team (NIST) to more efficiently support time-sensitive requests. The graphic below illustrates the interdependencies and intelligence flow during crisis.[7]

Organizational Milestones		Oversight & Key Reports
• President Roosevelt establishes the Office of Strategic Services (OSS)	1942	
• National Security Act of 1947 establishes the National Security Council and the Central Intelligence Agency	1947	
• National Security Agency established	1952	
	1956	• President Eisenhower establishes the President's Board of Consultants on Foreign Intelligence Activities
• Defense Intelligence Agency established	1961	
	1976	• Senate establishes permanent Select Committee on Intelligence (SSCI)
• President Carter signs EO 12036, reshapes the intelligence structure	1977 1978	• House establishes permanent Select Committee on Intelligence (HPSCI)
• President Reagan signs EO 12333, which clarifies previous orders and sets clear goals for the IC	1981	• President Reagan reconstitutes the President's Foreign Intelligence Advisory Board (PFIAB)
• National Imagery and Mapping Agency established	1996	• "Preparing for the 21st Century: An Appraisal of U.S. Intelligence"[8] • "IC21: The Intelligence Community in the 21st Century"[9]
• Intelligence Community Reform Act establishes ADCI for Collection and ADCI for Analysis & Production	1997	• "Report of the Commission on Protecting and Reducing Government Secrecy"[10]
	1998	• Commission to Assess the Ballistic Missile Threat to the United States[11]

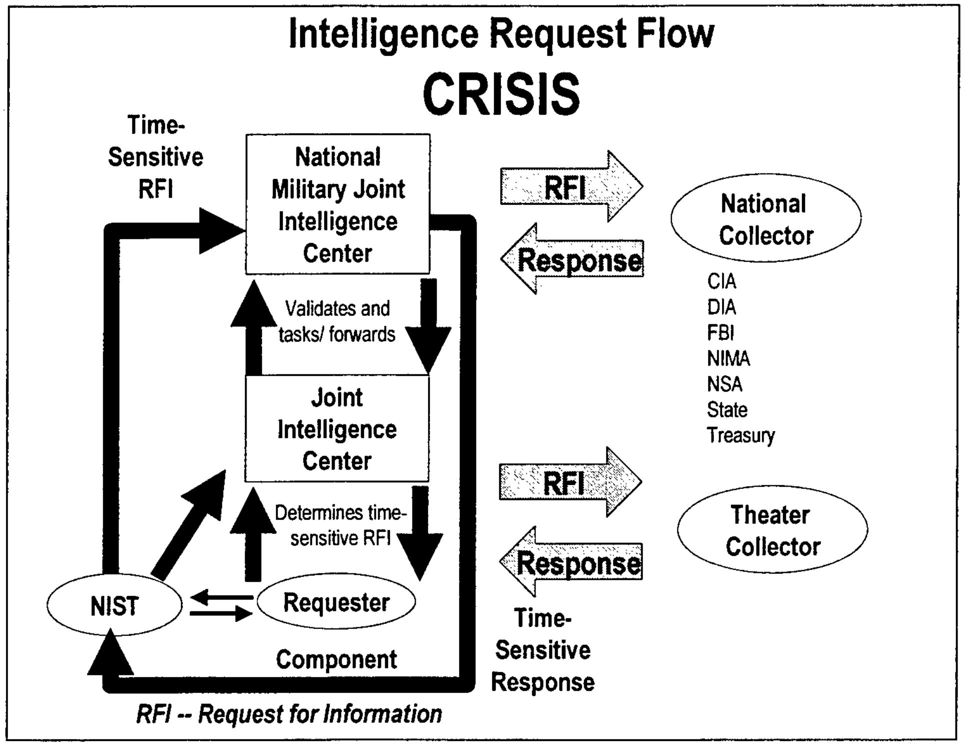
[7] "National Intelligence Support to Joint Operations", Joint Pub 2-02, 28 September 1998.

[8] "Preparing for the 21st Century: An Appraisal of U.S. Intelligence," Report of the Commission on the Rolés and Capabilities of the United States Intelligence Community, Washington, D.C.: U.S. Government Printing Office, 1996.

[9] "IC21: The Intelligence Community in the 21st Century," Permanent Select Committee on Intelligence, House of Representatives, 104th Congress, Washington, D.C.: U.S. Government Printing Office, 1996.

[10] "Report of the Commission on Protecting and Reducing Government Secrecy", Pursuant to Public Law 236, 103rd Congress, http://www.access.gpo.gov/int

[11] Unclassified Version of Intelligence Side Letter, Commission to Assess the Ballistic Missile Threat to the United States, March 18, 1999.


Intelligence Request Flow
CRISIS
Time-Sensitive RFI
National Military Joint Intelligence Center
Validates and tasks/ forwards
Joint Intelligence Center
Determines time-sensitive RFI
NIST
Requester
Component
RFI
Response
National Collector
CIA
DIA
FBI
NIMA
NSA
State
Treasury
RFI
Response
Theater Collector
Time-Sensitive Response
RFI -- Request for Information

The DoD clearly is a major stakeholder in the full spectrum of intelligence activities. The central question for this task force was:

> ***As we enter the 21st century, will our intelligence apparatus be postured to enable the DoD to successfully execute the National Military Strategy and achieve the goals outlined in Joint Vision 2010?***

Given the complex governance of the Intelligence Community and its interdependence with DoD-controlled programs, we found it necessary to take a broader view and to develop recommendations that extend beyond the sole purview of the Secretary of Defense. ***This task force concluded that "tinkering at the margins" is inadequate and that today's intelligence apparatus is incapable of effecting the necessary transformation in the absence of altered boundary conditions.***

STUDY APPROACH

"A sensible man never embarks on an enterprise until he can see his way clear to the end of it."
Aesop Fable, ca. 550 B.C.
"Look Before You Leap"

The study approach adopted by this task force was first to examine the anticipated 21st century threat environment, with particular emphasis on how the threats and adversaries are changing in the post-Cold War era. We then worked to characterize the future intelligence customers' needs, again emphasizing how the global security environment is altering both needs and expectations. Finally, we developed a high-level view of the strategic posture of the IC and its ability to meet the needs of its primary DoD customers. In an effort to better focus our study, we more closely examined two areas where we believe the intelligence requirements will be particularly stressing: expeditionary operations and homeland defense. Our recommendations are focused on better positioning the IC to meet the evolving demands of its diverse customer base.

In developing our understanding of the 21st century threat environment, we heard briefings from a number of IC components and related organizations.

- Mr. Ken Knight, Defense Intelligence Agency, emphasized the turmoil and uncertainty both today and in the future during his briefing entitled "Global Overview 1999-2019: Threats and Challenges in the Decades Ahead."
- Mr. James Detjen, Office of Naval Intelligence (ONI), described a shift from threat-based assessment towards capabilities-based assessments to drive the Navy's planning and acquisition processes.
- Major General John Landry (Ret.), National Intelligence Council (NIC), provided a threat briefing that addressed both global trends and military trends in the 2010-2015 timeframe.
- Mr. Roy Evans, MITRE, emphasized the need to strengthen our competency in gaining an understanding of the plans and intentions of our adversaries, arguing that sophisticated technology-based capabilities will be increasingly available worldwide.
- Mr. Doug Perritt, Deputy Director, National Infrastructure Protection Center (NIPC), provided an overview of the terrorist threats to our critical infrastructures.
- Major General John Campbell, USAF, Commander, Joint task force for Computer Network Defense, described the challenges confronting their team.
- Dr. Jim Bruce, Deputy National Intelligence Officer for Science and Technology, described the IC perspective regarding foreign science & technology programs.

Our early focus on intelligence needs for expeditionary operations and homeland defense led us to solicit customer views from several operational entities, including the United States Special Operations Command (USSOCOM) and the United States Atlantic Command (USACOM). The briefers described not only the intelligence needed, but also provided their view of the IC's ability to deliver.

- Rear Admiral Tom Steffins, USN, USSOCOM, emphasized the precision of the intelligence needed to effectively execute the missions of the Special Operations Forces.
- Major General Greg Gile, USA, USACOM, provided an overview of the emerging DoD mission in support of civilian agencies for Weapons of Mass Destruction (WMD) consequence management.
- Dr. Don Kerr, FBI, discussed the Bureau's role as a member of the IC and where their responsibilities are distinctly different due to their primary mission of law enforcement.
- Lieutenant Colonel Dave Castillo, USAF Cyberwatch, provided two briefings that focused on the challenges of providing strategic warning of potential offensive information warfare operations against the United States.
- We also benefited from the description of the Urban Warrior experiments by Brigadier General Donovan, USMC Warfighting Laboratory.

We augmented the briefings with task force discussions regarding the intelligence needed to effectively support JV2010 and the National Military Strategy.

To develop a view of the current posture and future strategy of the IC, we pursued several avenues. In addition to customer perspective, we solicited views from IC organizational leaders in key positions. We also heard from individuals who have recently been in a position to evaluate some portion of the IC's performance against critical issues. And, because skilled people are such a critical performance enabler, we solicited comments from a consultant who specializes in workforce issues.

- Ms. Joan Dempsey, Deputy Director of Central Intelligence for Community Management, described the role of the Community Management Staff and the status of major IC programs.
- Dr. Steve Cambone, National Defense University, summarized the findings from the Commission to Assess the Ballistic Missile Threat to the United States led by the Honorable Donald Rumsfeld.
- Mr. John Gannon, Chairman, National Intelligence Council, provided an overview on the state of health of the analytic elements of the IC.
- Lieutenant General James Clapper, USAF (Ret.), summarized major elements from his DIA-sponsored Human Intelligence (HUMINT) study.
- Ms. Helen Mills, AON Consulting, gave a perspective on changing workforce attitudes and organizational responses.

We augmented this work by reviewing the studies and reports which are referenced in the footnotes of the report.

In crafting this report we have opted not to directly link findings and recommendations. Instead, Chapters 4 through 7 discuss the major observations and findings, and Chapters 8 through 13 contain the task force recommendations. During the course of our study it became clear that the rapidly advancing and increasingly global technology environment – fueled by the explosion in information technologies – has an impact on every aspect of the business of intelligence. We therefore begin our report with a brief description of the major technological drivers that are defining the strategic context for 21st century intelligence.

STRATEGIC CONTEXT

"There is no reason for any individual to have a computer in their home."

Kenneth Olsen, 1977
President & Founder of Digital Equipment Corporation

The technology-driven, information-rich global environment is enhancing our adversaries' abilities to threaten our nation's interests and is expanding both the needs and expectations of the IC's customers. The same technologies simultaneously challenge the traditional ways of conducting the business of intelligence and provide new enabling tools and collection opportunities. Technology trends – driven in large measure by the Internet – are creating dichotomies in virtually every dimension.

The Internet is reshaping societies and fueling the global economy. During the decade from 1988 to 1998, more than 190 countries connected to the global network. In that same decade, the number of host machines connected to the Internet grew by more than 650 percent. And since the World Wide Web (WWW) was released by the European Laboratory for Particle Physics – CERN – in 1991, the number of web servers has grown to more than 7 million. This phenomenon is driving societal change – increasing openness and real-time communications – worldwide:[12]

- Malaysian Prime Minister Mahathir Mohamad, PLO Leader Yasser Arafat, and Philippine President Fidel Ramos met for 10 minutes in an online interactive chat session on January 17, 1996.
- In 1996, Saudi Arabia confined Internet access to universities and hospitals; Internet access became available to the Saudi Arabian public in January 1999.
- The Web became a focal point for British politics in May 1999, when a list of MI6 agents was released on a U.K. Web site.
- China's ChinaCast signed with Hughes Network Systems to help provide wireless broadband Internet services to businesses across China; 800,000 are expected to sign up in 2000.[13]
- The Indonesian government faced international pressure to ensure that the vote in East Timor, which allowed the Timorese to choose their own future for the first time, was free and fair; there was extensive online coverage of the evolving situation.[14]

[12] Hobbes' Internet Timeline. Copyright c 1993-9 by Robert H. Zakon. http://www.isoc.org/zakon/Internet/History/HIT.html

[13] "Hughes Signs Broadband Satellite Deal in China." Neil Taylor. *IT Daily*, August 30, 1999. http://asia.yahoo.com/headlines/310899/technolgy/936029460-135553.html

[14] "Internet Update Asia Special: East Timor Vote." Adam Creed. *Newsbytes*, August 30, 1999. http://asia.yahoo.com/headlints/300899/technology/936005280-135539.html

While countries worldwide are benefiting from the wealth of information and services available via the Internet, the same global information environment creates new vulnerabilities and arms our adversaries with additional means to threaten U.S. interests.

- In 1999, the first large-scale cyberwar took place simultaneously with the war in Serbia/Kosovo.[15]
- A forged Web page made to look like a Bloomberg financial news story raised shares of a small technology company by 31 percent on April 7, 1999.[16]
- “Cosmos’ Underground” provides links to hacking tools, “for educational purposes only” according to the home page, and invites the user to complete the “Hacker’s Manifesto.” (http://www.eden.com/~cosmos/ug/underground.html)
- “Onyx Dragon’s guide to explosives” provides directions for creating a “Shotgun Grenade,” an “Apple Bomb,” and an “Anti-person bomb.” (http://www.totse.com/files/FA031/bombz.htm)
- “The Chemical/Biological/Nuclear Anti-Terrorism” site provides a variety of links to related materials. (http://www.mindspring.com/~nbcnco)

The roots of today’s Internet can be traced to the U.S. response to the U.S.S.R. launch of Sputnik, but there was early engagement on the international scene. In fact, one of the most significant technological advances, creation of the World Wide Web, originated in Switzerland. Key events in the history of the Internet are shown below.[17]

Technological Progression		International Engagement
• USSR launches Sputnik; in response, Advanced Research Projects Agency (ARPA) formed within DoD to establish United States lead in military-related science and technology	1957	
• Leonard Kleinrock, MIT, authors first paper on packet-switching theory • ARPA sponsors study on “cooperative network of time-sharing computers” • ARPANET commissioned by DoD	1960	• National Physical Laboratory (NPL) in England develops experimental packet-switching network
• Ray Tomlinson, BBN, invents email • ARPA study shows 75% of ARPANET traffic is email • First demonstration of Internet protocols	1970	• French effort to build its own ARPANET • First international connections to ARPANET (England & Norway) • Elizabeth II, Queen of the United Kingdom, sends email from Malvern

[15] Hobbes’ Internet Timeline.

[16] Ibid.

[17] Ibid.

• ARPANET grinds to complete halt due to accidentally propagated virus • Desktop workstations come into being • NSFNET created; enables explosion of connections, especially universities • Internet worm burrows through net; CERT formed by DARPA	1980	• EUnet links Netherlands, Denmark, Sweden and UK • Stuttgart and Korea are connected • Canadian universities connected coast-to-coast • Email between Germany and China
• World Wide Web released by CERN • WWW proliferates at 341,634% annual growth rate of service traffic • CompuServe, America Online, Prodigy begin to provide Internet access • Electronic postal stamps become reality • Free computers are the rage (as long as you sign a long-term contract for Net service)	1990	• United Nations comes online • Japanese Prime Minister online • Hong Kong police, in search of hacker, disconnect 10,000 from Internet • Canada launches next generation Internet • Indian ISP market is deregulated • First large-scale cyberwar simultaneous with war in Serbia/Kosovo

It is important to note that the most dramatic changes on a global level have occurred within the past decade – that is, since the end of the Cold War – and were stimulated by the World Wide Web. This is of particular concern because this same era has been a time of diminished investment across the board – including both technological investment and personnel skills enhancement – within our intelligence apparatus. So just when retooling was desperately needed to cope with the exploding technological advances, resources were constrained and increasingly dedicated to maintenance and operation of legacy systems and capabilities.

It is equally important to recognize that "catching-up" to today's world is insufficient. In fact, the pace of technology-driven change appears to be accelerating. An increasingly popular calibration is the notion of a "web-year" – the equivalent of three months. In those terms, the year 2010 is 41 web-years away! Given the current rate of change, it is difficult to predict the future except by describing trends and themes. Looking to major technological drivers in the next decade, relevant "agenda-setting" themes include:[18]

[18] "Some Thoughts on Information Systems and Technology for the Next Decade and Beyond," George H. Heilmeier, Chairman Emeritus and former Chairman and CEO, Telcordia Technologies, formerly Bellcore.

Image processing	→	**Image understanding**
Search and retrieve • Based on keywords	→	**Concept/context search** • Question-and-answer
Text-based search	→	**Text, audio, picture search**
Data collection	→	**Knowledge extraction**
What you *ask* is what you get	→	**What you *need* is what you get**
Password/authentication-based security (access)	→	**Policy-based security** • **Adaptable/flexible response to attempted penetrations**
Wireline networks	→	**Wireless "everything"** • **Portability and mobility theme**
"Middleperson" as information hoarder	→	**"Middleperson" as information organizer, interpreter, filter**

In the next three sections, we describe how these major technological trends are creating new demands – both challenges and opportunities – and shaping the operating environment for the intelligence apparatus.

THREATS AND ADVERSARIES

" . . . *we must anticipate that future adversaries will learn from the past and confront us in very different ways*. . . "

Report of the National Defense Panel
December 1997

We are entering the 21st century in a position of uncontestable military dominance. This situation is expected to continue for the foreseeable future, because it is unlikely that our adversaries will invest the time and treasure that would be required to surpass our military superiority. At the same time that we have achieved global military dominance, we also have cast a broad commercial shadow that has enabled the United States to use trade as a weapon in a way that has never before been possible. In light of our overwhelming military and commercial power, a direct attack upon the United States would draw such a prohibitive response that no rational nation would consider such a move. We have thus driven our national and transnational adversaries to exploit asymmetric means. Further, this motivates our adversaries and potential adversaries to adapt to our current situation and vulnerabilities at the time of conflict. A key aspect of coping with this threat environment is identifying how our vulnerabilities might be exploited and what observable data could be collected to help prepare for such attacks. A direct, conventional attack on our geographic homeland – while possible – is far less likely.

There is a spreading instability in many regions of the world. Nationalism, religious fundamentalism, ethnic hatred, arbitrary borders, criminal activity on a global scale, and abject poverty have created fertile ground for groups inimical to the interests of the United States. With no homeland to defend, no fixed assets to preserve, and immunity to the consequences of failure, these groups are increasingly aware that the United States can be targeted anywhere in the world as long as the means employed blend with the background of normal human activities. Simply put, the vital interests of the United States cannot be bounded geographically. The same enormous commercial footprint that contributes to our global dominance has created organic dependencies between our economic stability and that of several unstable regions of the world. If one sets aside the emotional impact, an attack against the oil fields of the Middle East could have equal or greater economic impact on our nation than a direct attack upon the home territory. With our military and commercial dominance has come increased exposure to the growing levels of antipathy toward the world's remaining superpower.

Beyond the transnational groups that may seek to impose their will upon the United States, even national competitors have options other than a direct confrontation with our armed forces. Regional powers can exert pressure on allies, on sources of commercial supplies, and on sensitive transportation channels such as canals, ocean straits, and pipelines. This pressure can influence us either because of its direct effect on our commercial networks, or it may affect us indirectly by its impact on our allies. It is true that we may be uncontestable in the traditional military sense, but we are far from unchallenged in the emerging world of regional powers, religious fundamentalists, and criminal organizations. With proper tactics, and increasingly available capabilities, these groups can exert significant pressure on the activities of the United States.

Regardless of whether we consider our adversaries to be national or transnational in nature, the well-publicized success of our modern weapons and intelligence methods has caused substantial behavioral changes among those who would challenge us. The very fact of our military power has motivated non-traditional methods of attack, while at the same time our omnipresent commercial network has created global vulnerabilities to such attacks. Our adversaries have begun to adapt to these realities.

- Aware of our imagery intelligence, national and transnational actors adjust movements to deny and deceive our overhead systems while simultaneously seeking the same sources of information because of their commercial availability.
- Aware of the effectiveness of our signals intelligence, adversaries are employing potent encryption to ensure the privacy of their own communications, and they are also increasingly aware of the power that such means could confer upon them.
- Aware of our intolerance for collateral damage, adversaries are mixing civilian and military populations and installations.
- Aware of our national aversion to casualties, adversaries are targeting more vulnerable non-military and civilian populations.
- Aware of poverty and instability in the former Soviet Union, adversaries – national and transnational – may have opportunities to obtain weapons of mass destruction *and* the skills to deploy them. This has the potential to enable even transnational adversaries to threaten consequences heretofore reserved to advanced nations.
- Aware of our legal system, which seeks to preserve the freedoms that have created this unique society, terrorists know that if they are reasonably discrete they can operate within the homeland with an astonishing degree of freedom.

This is a wholly new challenge to our national security apparatus; our military forces are not ideal for this new world. Shaped as they were to win the Cold War, our armed forces are blunt weapons designed to be used against massed forces of an enemy who has a vested interest in minimizing the physical destruction of his forces and his homeland.

Our intelligence assets are likewise designed to ferret out the intentions and capabilities of a nation by enabling us to employ remote, sophisticated, technical means. Like the military forces they support, these means are not well-matched to a world wherein our enemies move like shadows to target embassies, computer networks, vital commercial supplies, and perhaps even the general population with biological or chemical weapons. Accustomed to a qualitative as well as quantitative edge in all encounters, we must be increasingly cautious as our adversaries access advanced technologies through commercial and criminal networks. Especially as it applies to intelligence, we will increasingly have to deal with adversaries who have an enormously expanded knowledge of us, while at the same time they have developed the sophistication to blunt, if not outright defeat, our most effective technical means.

This then is the environment in which the DoD must plan for the defense of the United States. We must act to protect vital – yet globally dispersed – interests. We must do this against a wide variety of adversaries who may have neither assets nor populations to protect. We must prepare to fight adaptive enemies; we must prepare to fight many of them. We must prepare to fight at home or for the proliferating vital interests that we have developed around the world.

National Adversaries

The emergence of nuclear-armed regional powers such as India and China, as well as the existing military capabilities of countries of the former Soviet Union, compels the United States to sustain capabilities to engage directly and overwhelm such threats. The military-to-military issues concerning such regional powers have been well-studied in the course of analyzing the requirements for prevailing in two major regional conflicts. But here again, these nations have options to pressure the United States that are less susceptible to ordinary military counter-moves.

The effects of the oil crisis in the 1970's or the Asian financial crisis in the 1990's are but glimpses of what a major regional power could accomplish by disrupting raw material supplies, interfering with normal transportation channels, or perhaps surreptitiously attacking the integrity of our computerized financial system. The restraint on such behavior is rationality. All of the above is possible, but at prohibitive cost to the nation that initiates the activities. The threat of retaliation can act as a substantive deterrent. There are those, however, for whom retaliation is not a credible option, and for them we must rely on prevention.

The Faceless Threat

As we confront an increasingly hostile world, we must not lose sight of the fact that the most effective attacks against our homeland in recent years have come from our own citizens, or legal aliens. The Oklahoma City and World Trade Center bombings were each carried out by residents of the United States. In many ways, the Oklahoma City bombing is more frightening because of its "justification." Wanton destruction was carried out by a small group of zealots who had no other objective than a wish to make known their hatred of the federal government. It is only in retrospect that motives for their actions can be discerned. The randomness of the target selection, the size of the group, and the legal protections the group enjoyed from preemptive surveillance paints a clear picture of the difficulty that an open society will have if it is to act to prevent, rather than retaliate for, homeland attacks.

The ability to preemptively attack the physical assets of society is compounded when we consider the impact of attacks against the computer infrastructure upon which we now depend. We rely upon the accuracy of our computer archives for all financial records, increasingly for medical records, transportation safety, and myriad other elements of our advanced civilization. Each and every one of these dependencies introduces new vulnerabilities. We have spent billions as a government – and more billions as corporations and individuals – to secure our critical sources of information and our access to them, yet we are routinely presented with evidence of intrusion by computer network attack or "hacker" groups. Even when we recognize that we are being penetrated, there is an additional complication: Is the penetration an organized attack by an adversary intent on causing harm, or is it merely a prank that has gotten out of control? That is, is it an attack on United States national security, or is it a law enforcement issue?

Given this situation at home, where our law enforcement authorities often have the networks in place to be sensitive to shifts in the public mood or in activities within groups known to be inimical to the government, how are we to protect our interests abroad? There, we have none of these advantages. True, we are not bound by some of the legal restraints that exist at home, but neither do we have the pervasive networks for penetrating and discerning the portents of an attack, nor do we have the discretion to take preventive action even if we were to suspect an imminent threat. The Khobar Towers attack in Saudi Arabia is a classic example where we were concerned about potential threats, but international agreement required us to negotiate our defensive perimeter with our hosts. Given our lack of freedom even when American lives were at stake, how much more restrained would we be if we were to discern a threat to the harbors and pipelines that provide the fuel for our industries? Such an attack, although not uniquely threatening the United States, would be far more disruptive to our economy than the recent African embassy bombings. The attack would be against a more dispersed asset and the attackers could well be legally entitled to access to these vital facilities – in spite of any reservations that the U.S. intelligence services may have! These situations would confront us with a two-fold challenge. It is considerably more difficult to get the essential elements of intelligence, and we may not have the freedom to act even on the intelligence that we do obtain.

The Narrowing Technology Gap

Much has been written in the last several years about the increasing military technology gap between the United States and other nations. Our advanced precision weaponry, supported by precision intelligence, has enabled us to strike at foes while minimizing the risk to ourselves and to surrounding civilian populations. While this situation is unlikely to change in the foreseeable future in terms of traditional military weaponry, we cannot afford to be complacent. Our adversaries are increasingly equipped with sophisticated technology-based capabilities that enable non-traditional attacks, such as biological or information warfare, and that enhance their abilities to observe our activities while concealing their own.

The arena in which we are most likely to incur a diminished superiority is intelligence. For a generation the United States had a near exclusive franchise for the worldwide collection of satellite-based imagery. We could act with great confidence that we knew much about our adversaries and they could know little about us. The coming availability of commercial imagery will make our military and commercial movements more transparent, while at the same time potential adversaries are taking effective action to counter our collection assets. The blind are about to see, and in seeing they will understand even better how not to be seen. Commercial imagery of our geographic homeland is already a commodity. It becomes difficult to imagine any advance that would restore the measure of superiority that existed when our adversaries were blind. We face the same two-edged sword in electronic intelligence. Even as we are being denied access to adversary networks due to encryption, the explosion of email, cellular, and fax communications is a tempting target for those who would exploit knowledge of us. Our adversaries, national and transnational, are aware and empowered.

Even the gap that has existed in weaponry is shrinking because of the increasing proliferation of high technology weapons sources. Economic collapse, and the rise of vast criminal networks, has created the potential of an arms bazaar in the states of the former Soviet Union. Weapons of mass destruction and the skills to use them may well be on sale – indeed sales have almost certainly taken place. The difficulties of dealing with chemical and nuclear weapons place some constraints on their use, but this is less true for biological weapons. Biological weapons have the added advantages that they are not only easy to manufacture and transport, but their effects may be manifest far removed in time and distance from where they were employed. And our nation's increasing reliance on the global information infrastructure – coupled with virtually instantaneous worldwide access to recipes for attack – provides potential adversaries with additional means to threaten U.S. interests. An adversary that does not fear retaliation has an incredible capability at his disposal.

In summary, we are in a time of transition. While JV2010 argues the increasing importance of stealth technology, the information age is redefining stealth from the physical to the virtual domain. Distinctions have blurred between:

- Peace and War
- National and International
- Foreign and Domestic
- Defense and Commercial

As concluded by the National Defense Panel: "Only one thing is certain: the greatest danger lies in an unwillingness or an inability to change our security posture in time to meet the challenges of the next century."[19]

[19] "Transforming Defense: National Security in the 21st Century," Report of the National Defense Panel, December 1997.

CUSTOMER NEEDS & EXPECTATIONS

"Great advantage is drawn from knowledge of your adversary, and when you know the measure of his intelligence and character you can use it to play on his weaknesses."

Frederick the Great
Instructions for His Generals, 1747

The ultimate objective of our intelligence apparatus is to enhance U.S. national security by informing policymakers and supporting military operations – that is, providing *knowledge of our adversaries*. Thus, policymakers and warfighters are the primary customers for intelligence, and success or failure of intelligence operations must be judged against their needs. It is an unfortunate reality that intelligence "failures" are too often exposed in the global media while successes necessarily remain uncelebrated. The recent bombing of the Chinese Embassy in Belgrade is but one example. Even so, few would dispute the fact that the IC continues to make significant contributions toward the protection of U.S. interests. In the aftermath of the bombings of U.S. embassies in Africa, IC efforts identified Usama Bin Ladin and his organization as the perpetrators. A number of other unclassified success stories are summarized in the DCI's *Annual Report for the United States Intelligence Community.*[20]

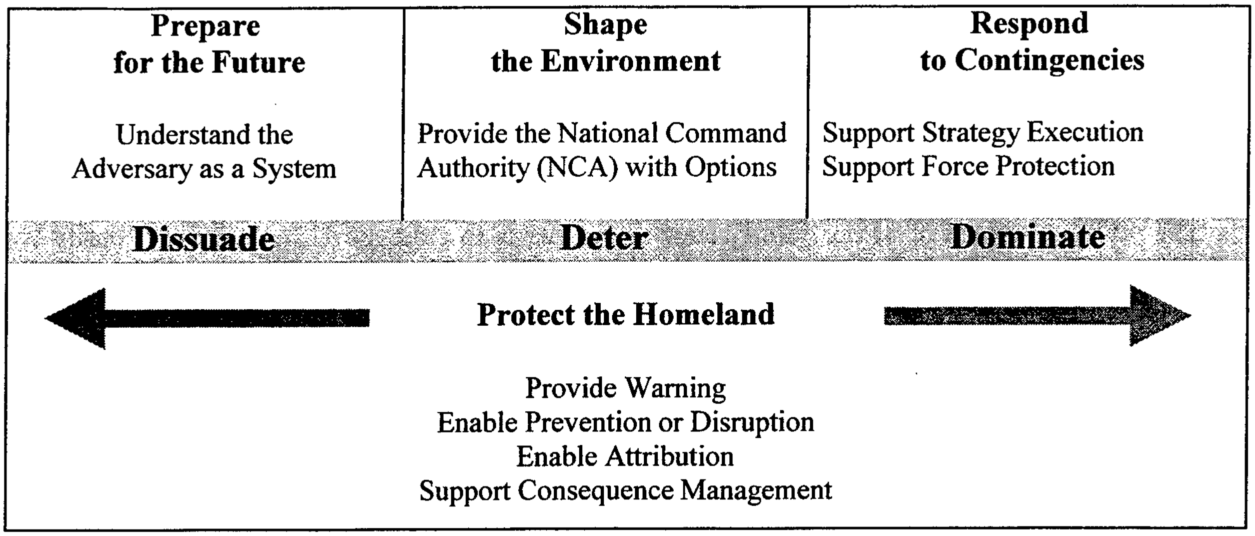
Customer needs for intelligence are being driven – in several dimensions – by the changing character of our adversaries and their abilities to threaten our interests. Customer priorities are increasingly dynamic and the issues of concern are expanding in diversity. Rather than focusing on a few major threats, the IC must continually analyze many potential adversaries. While timelines within which the IC must respond are shrinking, the need for greater precision and detail is growing. And while the need to protect sensitive sources and methods is unchanged, virtually every action taken by U.S. warfighters and policymakers is executed in a combined environment – driving the demand for more sharing of intelligence products with our coalition partners – or state and local officials in the case of homeland defense.

At the same time, customer expectations are being shaped by the technology-enabled, information-rich global environment. DoD customers increasingly rely on information networks and databases to enable their operations. Information provided by the IC is of limited value unless it is readily accessible within their electronic operating environment. All customers have a wealth of relevant information at their fingertips as well as the ability to apply sophisticated, commercially available tools to help them mine that information space. There is a growing desire by key customers to have the option to customize their information ensemble – to meet their individual needs – rather than receive standard reports and serialized products. Customers' opinions are generally shaped by what they learn from the information-rich open source environment – driving the need for the IC to put their unique information and analytic judgments into this broader context.

Intelligence has been described as *knowledge that reduces risk or uncertainty for decisionmakers*. Whether a warfighter or a policymaker, effective intelligence is critically important throughout the full spectrum of peace, crisis, and war. To more fully characterize the

[20] "Annual Report for the United States Intelligence Community." http://www.cia.gov/publications/fy98intellrpt/foreward.html

customer needs for intelligence, we developed a model based on the key themes of the National Military Strategy.



Prepare for the Future	**Shape the Environment**	**Respond to Contingencies**
Understand the Adversary as a System	Provide the National Command Authority (NCA) with Options	Support Strategy Execution Support Force Protection
Dissuade	**Deter**	**Dominate**

Protect the Homeland

Provide Warning
Enable Prevention or Disruption
Enable Attribution
Support Consequence Management

In simplistic terms, the top of the chart focuses on issues external to the United States, while the bottom is internally focused. Our intelligence apparatus is expected to meet the needs of its policymaker and warfighter customers across this diverse spectrum of objectives. At any given time, different customers will be dealing with different issues and objectives – of varying relative priorities – but all are important.

PREPARE FOR THE FUTURE

As stated in our Terms of Reference, intelligence customers need "adequate warning, with specifics, of developing military and technology capabilities which could threaten national security." We foresee a 21st century environment in which our adversaries are better informed – of our capabilities *and* vulnerabilities – and better equipped with sophisticated weaponry and support systems. It seems inevitable that many potential enemies will have access to weapons of mass destruction (WMD) and the means for deployment. It is equally apparent that our adversaries are gaining a good understanding of the vulnerabilities of our information networks and critical infrastructures – from the constant media attention, if by no other means. And our adversaries have yet another tool at their disposal – the ability to influence U.S. public opinion and potentially shake confidence in our national security establishment. Intelligence customers are already confronting many of these issues, and their demands are stressing today's intelligence apparatus. We anticipate customer needs to continue to grow as we enter the 21st century.

Effective decision making in this evolving global environment requires a holistic understanding of our potential adversaries. We must know not only their military and technology capabilities but also their motivations and intentions. We must understand the cultures and moral codes that motivate and guide their behaviors. We must know their friends and allies – those who would enhance their abilities to threaten U.S. interests or provide sanctuary. Like the United States, our adversaries are increasingly dependent upon the global commercial infrastructures, as enablers to their operations and as international environments within which their actions are more readily concealed. We must know their dependencies and their vulnerabilities, in the physical as well as in the virtual domain. We must understand our adversary as a *system*. With such an understanding, we will gain new insight into information linkages and interrelationships – permitting meaningful correlations among disparate databases and enabling us to more effectively mine the global information environment.

SHAPE THE ENVIRONMENT

U.S. military forces have historically helped shape the international environment through their deterrent qualities as well as through peacetime military engagement. Key elements of this component of the National Military Strategy include:

- Promoting Stability
- Preventing or Reducing Conflicts and Threats
- Peacetime Deterrence

Each element has implications for intelligence support.

Global stability is promoted through peacetime engagement activities, such as combined exercises, to enhance interoperability and readiness, and sharing of information. Current and future coalition actions involve international partnerships that extend well beyond our traditional allies. And these partnerships are increasingly situational in character – that is, a partner in one action may be an adversary with regard to other intelligence issues. The challenge for our intelligence apparatus is to maintain the delicate balance between supporting our national desire to enhance global stability while not further diminishing the value of our intelligence assets through international exposure.

The IC plays a key role in supporting diplomatic and policymaker efforts to prevent or reduce conflicts and threats. In the world today, regional conflicts are often fueled by religious or ethnic differences. Many foresee a 21st century environment in which conflicts increasingly stem from changing demographics, diminishing natural resources, and other socio-economic drivers. New challenges are emerging as we seek to establish – and verify – arms control agreements to limit the development, possession, and use of chemical and biological weapons. Effective intelligence support will require not only a robust understanding of the changing global environment, but also the ability to collect against the new observables relating to proliferation of WMD capabilities and other emerging threats.

Historically, our deterrence strategy has been embodied by our demonstrated ability and willingness to engage and defeat aggression. While this component remains viable for some circumstances, the 21st century global environment will demand multi-faceted deterrence strategies. Richard Danzig suggests that we employ the art of *dissuasion* as an element of our strategy to shape the international environment.[21] The recent agreement by North Korea to cease their test-firing of long-range missiles as long as talks with the United States continue could be characterized as successful application of the art of dissuasion. In any case, given the emergence of asymmetric capabilities – biological, chemical, and information warfare in particular – it is clear that we must redefine deterrence.

Adaptive adversaries with increasingly sophisticated capabilities have altered the rules of the game, and this will place new demands on our intelligence apparatus. At the same time, the global technology environment offers new opportunities for active options – for use by our National Command Authority (NCA) – that could yield a more robust 21st century deterrent strategy.

RESPOND TO CONTINGENCIES

Each of our military services has defined strategies to develop the requisite weaponry, operational infrastructures, and personnel skills to enable them to effectively execute expeditionary operations. There is equivalent focus on this mode of warfighting – and in conducting "operations other than war" (OOTW) – in the joint community. In fact, JV2010 anticipates that deployment of huge complements of massed forces will be the exception in 21st century conflict. While our current force structure was designed with the capacity to simultaneously fight two major theater wars, it now appears more likely that our military forces will be simultaneously engaged in multiple contingencies. The need to effectively support a number of simultaneous military engagements places additional pressures on our intelligence apparatus.

Precise and detailed intelligence is required to support NCA strategy execution in any military operation. As was demonstrated by the events in Kosovo, our precision weapons are quite effective – if the intelligence guiding them is equally precise. But the need for precision extends beyond geospatial information – it must include the temporal dimension. We expect that 21st century adversaries will increasingly adopt the strategy of intermingling civilian and military populations and installations. Such situations will require precise understanding of the local conditions – including mobile targets, weather conditions, surrounding population, patterns of activity, and so forth. This means the local commander must have the ability to task our intelligence apparatus – both in preparation for attack and to assess the effect of an attack – and receive a response in near-real-time. It will be equally important to understand the cultural beliefs and moral codes that govern the behavior of our adversaries, and the critical infrastructures that enable their operations – and make them vulnerable. If we have done our homework, and *understand our adversary as a system*, our deployed military forces will have a tremendous advantage.

Force protection is an equally challenging element of our national strategy, particularly for expeditionary operations. By their very nature, these forces are rapidly deployed, smaller, lighter units. As a result, they need advanced intelligence to ensure that they deploy with the necessary protective gear – especially if they are likely to confront an adversary possessing WMD

[21] "The Big Three: Our Greatest Security Risks And How to Address Them," Richard Danzig, Copyright Richard Danzig 1999.

capabilities. And during deployment it is vitally important that their support infrastructure – their supply of information and sustenance – be protected from local threats.

From an intelligence perspective, the increasing engagement in coalition operations brings with it extremely stressing security issues. Our military forces need integrated and interoperable systems to effectively conduct combined operations – this includes their command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) systems. This combined operational environment suggests the need for a dramatically different way of thinking about information security, and protection of sensitive sources and methods – since coalition partners vary according to the situation at hand.

Many of these 21st century intelligence drivers can be derived from the operational concepts described in JV2010:[22]

- Dominant Maneuver
- Precision Engagement
- Full-Dimensional Protection
- Focused Logistics

While not made explicit in the document, each concept has significant implications for our intelligence apparatus.

PROTECT THE HOMELAND

Protecting our homeland, while of growing concern to the public and government alike, is an area fraught with challenge. How will we distinguish a threat to our nation's security from a criminal attack – or possibly a juvenile delinquent hacking into our information infrastructure? Is our "homeland" geographically bounded, or does it extend to U.S. interests worldwide? How would we provide *indications and warning* (I&W) for a biological attack in downtown Washington? There are domestic civil liberty concerns as well – the difference between a terrorist and a freedom fighter is often a matter of perspective. Challenges span the spectrum from legal and jurisdictional issues to the abilities of our intelligence apparatus to equip our decisionmakers with the requisite information to enable them to warn, prevent, disrupt, or attribute, and manage the consequences in the aftermath of an attack.

An attack on our homeland could take a variety of forms. It could be a lethal or non-lethal attack to delay, disrupt, or debilitate our warfighting ability. In the case of a ballistic missile attack on a U.S. military installation, roles and missions are quite clear – as are the customer needs for intelligence. The picture is less clear, however, if terrorism or psychological warfare is employed to diminish national will, or if attacks are intended to disrupt or diminish the ability of our government to function. And roles and responsibilities are even less clear in the case of an infrastructure attack that results in a loss of confidence in our financial system. Although the National Infrastructure Protection Center is working this problem, in today's legal framework, an attack – when detected – is first assumed to be a law enforcement matter rather than a threat to

[22] "Joint Vision 2010," John M. Shalikashvili, Chairman of the Joint Chiefs of Staff.

our nation's security. Former House Speaker Newt Gingrich, a member of the United States Commission on National Security for the 21st Century, recently predicted that new threats from WMD could require the United States to implement a "capability of homeland defense on a scale never dreamed of and [that] will require a significant redistribution of authority and power."[23]

The structure of the U.S. response to terrorist threats inside the United States is now emerging, at least in theoretical form. To dramatically oversimplify a complex network of responsibilities:

- The FBI is responsible for events up to an attack; Federal Emergency Management Agency (FEMA) is responsible for consequence management after an attack. The National Guard will play a role at the state level in early response to attacks. First responders – fire departments, police, hazmat teams – will generally arrive on the scene before any other officials.
- The DoD will support these activities if required, and will probably develop technology for use in homeland defense; the Department of Energy (DOE) will also build technology for homeland defense.
- Other federal and state agencies, especially Health and Human Services (HHS) and the Department of Agriculture for biodefense, will also play important roles.

All are, in principle, customers for intelligence.

Many of these groups have not previously worked with one another, and there are no well-defined mechanisms for sharing information. Concerns with secrecy, and with the protection of collection sources and methods, strongly inhibit full sharing of information. The questions of how and to whom to provide information, at what level of completeness and secrecy, and in what form in order to be interpretable and useful, all remain largely to be resolved. These questions, however, are not unlike some of the issues confronted in providing effective intelligence support to coalition warfare.

As the task force examined the concept of homeland defense against threats such as chemical, biological, or other forms of terrorism, it became clear that no single entity of the U.S. government is charged with developing and prioritizing intelligence needs. Further, no single combatant command is charged with developing plans for a military response to threats directed against the U.S. homeland, whether from state- sponsored groups, non-state actors, religious or ethnic hate groups, or individuals. Current laws and executive orders, specifically *posse comitatus* and rules governing the collection of intelligence about U.S. persons, have served us well in the past. However, it may now be prudent to review the provisions that restrict the activities of the active armed forces and the intelligence community in domestic emergencies, in light of new threats.

The report of the National Defense Panel argued that coastal and border defense of the homeland – not seriously considered since the late 1950s – is a challenge that again deserves serious thought.[24] It further states that "better coordination between those national agencies charged with gathering intelligence outside our borders and with those charged with protecting our citizens and territory will be an absolute requirement."

[23] "Security State?", Defense Daily, Monday, September 20, 1999.

[24] "Transforming Defense: National Security in the 21st Century," Report of the National Defense Panel, December 1997.

STRATEGIC POSTURE

"The inability to predict the Indian Nuclear tests in May 1998 was a clear sign that the Intelligence Community needs to evaluate available resources, technology, and techniques against the threats facing us today."

DCI Annual Report[25]

A number of reports, studies, and assessments conducted during recent years have expressed significant concerns regarding both current performance of the IC and its ability to adapt to the emerging needs of our national security apparatus.

In "Preparing for the 21st Century: An Appraisal of U.S. Intelligence," the Commission on the Roles and Capabilities of the United States Intelligence Community observed the need for:[26]

- Better integration of intelligence into the government communities it serves, acknowledging the need for more specific direction to the IC from its customers
- Intelligence agencies to operate as a "community," arguing that the current arrangement lacks strong central direction
- Creation of greater efficiencies with more rigor and application of modern management practices, noting that the costs of misaligned workforces prevent the investment in needed technical capabilities and initiatives

In "IC21: The Intelligence Community in the 21st Century," the authors argued:[27]

- That the IC is a product of the Cold War environment; it does not represent the array of organizations, capabilities, and processes that would be designed if we were starting from scratch today
- The need for IC "corporateness" as an overarching concept, including strong central management by the DCI and a Director of Military Intelligence (DMI) with strengthened authority over military intelligence
- That the military objective of "dominant battlespace awareness" would require significant advances in technology, development of consolidated requirements, coherent tasking management, and synergistic intelligence collection capabilities

The Rumsfeld Commission, chartered to assess the ballistic missile threat to the United States, observed that the IC's ability to provide timely and accurate estimates of ballistic missile threats to the United States is eroding. Particular concerns included:[28]

[25] "Annual Report for the United States Intelligence Community." http://www.cia.gov/publications/fy98intellrpt/foreward.html

[26] "Preparing for the 21st Century: An Appraisal of U.S. Intelligence," Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, Washington, D.C.: U.S. Government Printing Office, 1996.

[27] "IC21: The Intelligence Community in the 21st Century," Permanent Select Committee on Intelligence, House of Representatives, 104th Congress, Washington, D.C.: U.S. Government Printing Office, 1996.

[28] Unclassified Version of Intelligence Side Letter, Commission to Assess the Ballistic Missile Threat to the United States, March 18, 1999.

- "The fact that so many of the requirements relate to the support of real-time operations – support to military and diplomatic operations, anti-drug and anti-nuclear smuggling, political analysis of unstable governments – assures that near-term operational issues will receive the greatest attention while longer-term strategic issues are left to be dealt with as time and resources may or may not permit."
- "The ballistic missile and WMD threats are not normally treated as a strategic threat to the United States, on a par with any other highest priority issues." Rather, these capabilities are viewed a contraband, and "attention is focused primarily on the process by which technology, techniques, and technicians are transferred from seller to buyer."
- "The decline in the IC's scientific and engineering competence is one of several recent developments which have adversely affected the performance of the IC on ballistic missile and WMD developments."

The recently published "Combating Proliferation of Weapons of Mass Destruction" also argued that "we do not have a comprehensive approach to combating the proliferation of weapons of mass destruction." [29] The report proposes creation of a "National Director for Combating Proliferation" and defines a comprehensive set of recommendations spanning the spectrum from leadership and policy guidance to clarification of roles and responsibilities and inter-agency relationships. Specific recommendations for the IC suggest that the intelligence apparatus is not well-positioned in a number of dimensions. Report recommendations identified the need to:

- Improve the intelligence presented in terms of responsiveness to and usability by the policymaker
- Apply clear standards of evidence to current intelligence and warning assessments, as well as longer term analyses and estimates
- Create a single proliferation-related intelligence program plan
- Ensure that there is integrated collection planning against priority proliferation targets
- Strengthen the proliferation-related analytical capabilities throughout the IC and assign lead responsibility for proliferation analysis
- Develop a multi-year plan to enhance the technical capability for proliferation-related intelligence collection
- Develop a process for resolving disputes regarding the use of proliferation-related intelligence

The DoD Combat Support Agency Review Team is currently completing its assessments of the performance and strategic posture of all Combat Support Agencies. Draft reports have identified a number of issues and concerns, including:

- Affordable solutions to support tasking, processing, exploitation, and dissemination of intelligence

[29] "Combating Proliferation of Weapons of Mass Destruction," Report of the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, Pursuant to Public Law 293, 104th Congress, July 14, 1999.

- Intelligence availability on collateral classified and unclassified networks to provide better access to operational users
- Development of tools to assist exploiters in target recognition and detection to speed the exploitation process
- Redressing of shortfalls in analytic skills – both strength and depth – in virtually every intelligence discipline as well as in the all-source community
- Strengthening of human intelligence (HUMINT) coverage
- Integrating collection management for all intelligence assets – both tactical and national
- Strengthening and integration of measurement and signature intelligence (MASINT) capabilities into mission planning and execution – particularly critical in light of emerging WMD-related threats

Concerns with the performance of the U.S. Intelligence Community are unlikely to diminish as we enter the 21st century. Instead, there is every reason to believe that the IC will be continually scrutinized as new problem sets develop – and additional "failures" occur – unless aggressive steps are taken to redress the conditions that impact its current performance. This task force is not suggesting that the IC components have been blind to the problems or oblivious to the many recommendations, only that the actions to date have made marginal improvements to a basically dysfunctional intelligence apparatus.

Personnel reductions – congressionally mandated, to be sure – coupled with technical advances in collection systems, have resulted in fewer and fewer analysts being tasked to produce more and more intelligence about an increasing array of topics. The Community is, to put it gently, in a reactive mode, responding to today's hot topic by reallocating scarce resources away from the proactive production of all-source intelligence to guide the daily actions of policymakers and warfighters. This has resulted in the establishment of various centers, theoretically dedicated to a single problem set. Unfortunately, there are no single problem sets anymore, and basic intelligence functions such as indications and warning, scientific and technical, and political intelligence are drained of analytic talent.

Today the U.S. intelligence apparatus is stressed in every dimension. It is relatively easy to understand how this situation came about when we consider the major happenings of the past decade. The collapse of the Soviet Union and the fall of the Berlin Wall fueled our national desire for a "peace dividend." This led to a decade of budgetary decline and constrained hiring across the entire national security community – including, but by no means confined to, the intelligence apparatus. Almost simultaneously, the World Wide Web hit the scene and the global information technology environment exploded. At precisely the time when the Intelligence Community needed to reinvent itself to cope with the realities of the changing global environment, it instead accommodated budget cuts by trading away investment – in people as well as in technology – to sustain operational capacity. Such a strategy can work – for a short time in a relatively stable operational environment. But it leads to disaster when the operational environment is changing or when the trades are extended for more than a brief period of time.

We have already argued that the global technology environment has an impact on every aspect of the intelligence business. But just as it is enhancing the capabilities of our adversaries and contributing to the increasing expectations of intelligence customers, it offers our IC the opportunity to transform its own capabilities. Mature and emerging technologies have the potential to enable more timely and robust support to the warfighter as well as to the policymaker. We *could* create an intelligence enterprise that would consistently leverage the best talent – regardless of physical location – together with all relevant information – regardless of source – to yield the greatest possible insights toward *Decision Superiority*. We *could* build new collection capabilities that would enhance the effectiveness of the intelligence apparatus against emerging threats and new observables. Unfortunately, the resource allocation processes, as currently executed, are unlikely to yield these lofty outcomes.

Many previous studies and reviews have noted the growing tension between readiness and modernization. In the absence of stable foreign policy and clear national priorities, the IC is driven to be "all things to all people." Performance against today's diverse suite of issues is due to motivated and committed personnel – *and in spite of systems and processes*. But the lack of investment impedes even today's performance, as illustrated by the absence of current databases defining the location of the Chinese Embassy in Belgrade. And, as evidenced by the findings of the Rumsfeld Commission, the community is not well positioned against emerging threats such as intercontinental ballistic missiles or weapons of mass destruction.

The U.S. Intelligence Community is, and has been since the end of World War II, purposefully oriented toward the detection of traditional military threats (e.g. weapons, weapon platforms, and forces) and the counting of such assets. This factor, more than any other, has forced the dominant share of intelligence resources to be spent on remote technical collection [signals intelligence (SIGINT) and imagery intelligence (IMINT)] at the expense of clandestine collection and comprehensive analysis. These legacy collection assets cannot meet the demands of today's increasingly diverse and dynamic national security environment; and their utility is limited against emerging threats.

The voice of the intelligence customer is inadequate in today's intelligence resource allocation process. Although customers have a role in establishing intelligence requirements, the path between their input and delivered intelligence is arduous and time-consuming. Programs are aligned and resources are allocated to collection stovepipes – the *means* – rather than to intelligence missions – the *ends*. Although the Community Management Staff attempts to optimize resource allocation across the programs, changes are, by their own admission, at the margins in the context of the overall intelligence budget. And even then it is unclear that the shifts are driven by response to clearly articulated customer needs. The current resource allocation process has several readily identifiable flaws:

- There is no end-to-end programmatic ownership of either intelligence systems or intelligence missions – leading to stovepipe-specific infrastructures with minimal integration across the intelligence enterprise. This situation impedes coherent support of customer needs from a tasking and dissemination perspective as well as robust collaboration from an analytic perspective.
- Because resources are allocated to existing programs, investments made during an era of tight resources tend to be focused on incremental enhancements of legacy capabilities. There is little chance that innovative or revolutionary capabilities will emerge from this environment. This is particularly true when potential new

capabilities do not fit within one of the major programs (SIGINT, IMINT, HUMINT) – as is the case with most WMD-related sensor technologies (e.g. MASINT).

- Although the Intelligence Community has recently begun to increase its investment in analysis, the analytic community, like the intelligence customer, has a weak voice in the resource allocation process. As a result, intelligence analysts are operating with an information infrastructure that lags today's commercial environment. Moreover, needed investments in data fusion, modeling and simulation tools, and other technological enablers are significantly under-funded.

Resource allocation authorities for the NFIP, which contains the largest share of the intelligence budget, are accorded to the Director of Central Intelligence by Executive Order 12333. The allocation process is, however, complicated by the fact that not only is the majority of the budget contained within the DoD appropriation for historic reasons of secrecy, but also by the fact that by far the largest share of the NFIP is executed by DoD components. In practice, the resource allocation process is driven by a complex set of committees and review groups. In the absence of a strong customer voice and robust *measures of effectiveness* (MOE) for each of the programs, there is little basis for radical resource shifts. As a result, the outcome is typically "tinkering at the margins" with little real impact.

FINDINGS: THE BOTTOM LINE

"Treating the threat as one of a hundred or more high-priority issues, all of which are placed on a back burner with each crisis and contingency that comes along, will not improve the capability of the IC to provide actionable warning."

Unclassified Version of Intelligence Side Letter[30]
Donald Rumsfeld, March 18, 1999

In geopolitical terms, there has been a shift from a bipolar world to a complicated global collage, with new and vastly different threats. The quantity of collectable data relevant to those threats is now very nearly overwhelming, and it will continue to grow in the future. But at the same time, we are not equipped to collect against critical emerging threats – such as biological, chemical, and information warfare. This shift in focus has given rise to *perceived* requirements on a scale never before imagined. It is no longer adequate to divide the world into geographical regions or to categorize military threats based upon order of battle estimates.

The situation is tenuous at best; analytic successes are likely to go largely unnoticed and generally be unrewarded, while intelligence failures will be spotlighted. Analysts are expected to understand issues involving religious and ethnic rivalries, the impact of natural resources on national policy, and the nuances of foreign internal political competition on international politics and trade. In addition to support for precision weapon systems, detailed intelligence is now required for humanitarian relief operations, peacekeeping, and non-combatant evacuations. The deployment of U.S. armed forces in a coalition environment has placed additional strains on our intelligence apparatus – demanding that it produce timely and meaningful products that can be released to various coalition partners. And the emergence of threats to our homeland stresses the intelligence apparatus in every dimension.

The 21st century national security environment will demand a fundamentally different set of intelligence skills, tools, and methodologies.

- Given that our warfighters must operate inside the ever-shrinking decision cycle of our adversaries, we must have a system in place to provide near real-time *precision intelligence* to guide their precision weapons – and the system must integrate the entire spectrum of tactical and national intelligence assets.
- Given that virtually all future actions will be executed with coalition partners, we must adopt a *need-to-share* – versus need-to-know – security paradigm, and ensure that the IC's products become an integrated contribution to the warfighter's customized information ensemble.
- Given the increasingly diverse threat environment and shrinking timelines, we must make collaboration and information sharing the norm – both internal and external to the IC. This will drive the need for a robust information infrastructure and a supportive *need-to-share* security paradigm.

[30] Unclassified Version of Intelligence Side Letter, Commission to Assess the Ballistic Missile Threat to the United States, March 18, 1999.

- Given the overwhelming quantity of data available on virtually every intelligence issue, we must robustly fund analytic capabilities in order to more effectively utilize the investments made in collection.
- Given that the IC is not a monopoly, analytic efforts must master the customer-accessible information space, integrate unique nuggets of intelligence, and produce shareable, timely, value-added judgments.
- Given that the time between first observation and deployable threat is likely to be short, we must routinely exploit modeling and simulation and scenario-based analytic methodologies to help anticipate what *might* happen and what signs would provide effective indications and warning for emerging threats.
- Given that our adversaries understand much about our legacy intelligence collection assets, we must focus on identification and collection of new observables – such as trails left in the global information infrastructure (e.g. commercial data documenting the international flow of sensitive technologies) – and close-in MASINT sensors.
- Given that more adversaries will have access to the means to threaten U.S. interests, we must strengthen our ability to discern *plans and intentions* – with particular emphasis on more robust understanding of other cultures and moral codes, and strengthened HUMINT collection capabilities.
- Given that the rapidly advancing global technology environment is enabling our adversaries – just as it has the potential to significantly enhance our own intelligence activities – we must improve the science and technology-related workforce skills in every component of the IC.

Because we are unlikely to return to an era where our national security apparatus is focused on a single dominant superpower – or even a stable family of threats – an effective 21st century intelligence apparatus will be:

- Robust against widely diverse issues, while maintaining sufficient depth on each to enable precision operations
- Agile amidst rapidly changing priorities, while maintaining vigilance over important strategic issues
- Anticipatory – able to forecast the important changes in global conditions
- Fully integrated with the customer communities it serves

RECOMMENDATIONS: A MODEL

"In all of our military institutions, the time-honored principle of "unity of command" is inculcated. Yet at the national level it is firmly resisted and flagrantly violated. Unity of command is endorsed if and only if it applies at the service level. The inevitable consequence is both the duplication of effort and the ultimate ambiguity of command."

Secretary James Schlesinger, 1983[31]

In crafting our recommendations, the task force considered a number of options. The notion of starting with a clean sheet of paper and designing an intelligence apparatus appropriate for the envisioned 21st century environment, although attractive, was deemed impractical from an implementation perspective. At the other end of the spectrum, recognizing the abundance of time and intellect that has been devoted by similar groups, there was the inevitable desire to simply select those previous recommendations with which we agreed and endorse them in this report – hoping that repetition would engender change. Our product is something of a hybrid of these options.

Rather than beginning with a clean sheet of paper, we chose to model our recommendations for the IC after major actions and initiatives within the DoD. While not claiming a perfect mapping, we believe that the challenges faced by the IC are not unlike the problems confronted by the DoD during the past two decades. And although we cannot argue that the actions taken have resolved all of the shortcomings within the DoD, we believe there are relevant lessons for the IC.

Beginning with the Goldwater-Nichols Department of Defense Reorganization Act of 1986, we identified significant parallels in terms of the background issues. This legislation was stimulated by a desire to create a more appropriate balance between joint and service interests and had eight broad purposes:[32]

1. To reorganize DoD and strengthen civilian authority
2. To improve the military advice provided to the President, National Security Council, and Secretary of Defense
3. To place clear responsibility on the commanders of the unified and specified combatant commands for the accomplishment of missions assigned to those commands
4. To ensure that the authority of commanders of unified and specified combatant commands is fully commensurate with the responsibility of those commanders for the accomplishment of missions assigned to those commands
5. To increase attention to strategy formulation and contingency planning
6. To provide for the more efficient use of defense resources

[31] United States Senate Committee on Armed Services, "Organization, Structure and Decisionmaking Procedures of the Department of Defense", hearings before the Committee on Armed Services, 98th Congress, 1st session, 1983-84, part 5, p. 187.

[32] "Taking Stock of Goldwater-Nichols," James R. Locher III, *Joint Forces Quarterly*, Autumn 1996.

7. To improve joint officer management policies
8. To otherwise enhance the effectiveness of military operations and improve DoD management and administration

We argue that numbers 2, 5, 6, and 8 have direct corollaries to IC deficiencies described in earlier sections of this report. We argue further that a major shortcoming in today's IC is the lack of an equivalent *joint* operational construct, which would then enable items 3, 4, and 7. Although implementation of the Goldwater-Nichols Act has perhaps fallen short of its original objectives in some areas, it is widely recognized as having a revolutionary impact on our defense establishment.

There are other DoD initiatives that have implications or lessons for the IC:

- The DoD is attempting to achieve interoperability of its full suite of C^4ISR assets – in both *joint* and *combined* operational environments. In light of limited success to date, USACOM is taking on the mission of integrating such systems for the operational environment. Our intelligence apparatus faces a similar need – for *jointness* within the IC, in *combination* with DoD and its coalition partners, and in *combination* with the various governmental entities responsible for homeland defense.
- The DoD initiated the Advanced Concept Technology Demonstration (ACTD) and similar programs to stimulate experimentation and development of new operational capabilities. The IC needs an equivalent mechanism to stimulate innovation and development of new capabilities – particularly across the seams between today's intelligence stovepipes.
- The DoD supports strategic investment – albeit on a reduced and probably inadequate scale – in both technology and personnel. Both the DoD and the IC face the dual challenge of retooling existing workforces while attracting and retaining the talent necessary for the future. And both also need to build and sustain technology investment strategies that focus on *breakthrough* technologies – those with the potential for revolutionizing their operations.

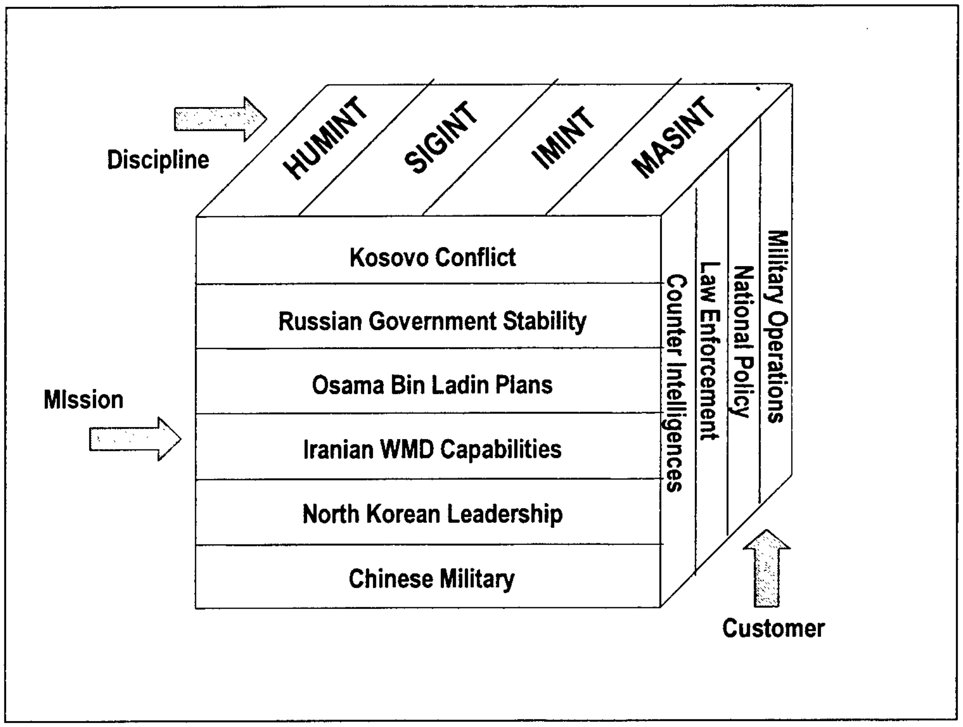
These broad elements constitute the DoD-derived model that was used to frame our recommendations, which are contained in the next four sections.

MISSION MANAGEMENT

"The intelligence community is less a community than a collection of more than a dozen largely autonomous components spread throughout the Washington, D.C. area and the world."

"Making Intelligence Smarter"[33]
Sponsored by the Council on Foreign Relations

The IC can be viewed – and must be effectively managed – from at least three different perspectives: national security mission; customer segment and intelligence discipline. For example, a mission might be to deter Chinese build-up of ballistic missile capabilities. Within that mission, specific customer segments – such as policymakers, military planners, and warfighters – would have differing but related needs for intelligence. And the various intelligence disciplines (HUMINT, SIGINT, IMINT, MASINT) all have information to contribute. In practice then, we are trying to optimize performance over a complex three-dimensional parameter space of missions, customers, and intelligence disciplines.



Today's IC is largely organized and resourced by intelligence discipline, and personnel incentives generally motivate individuals to produce discipline-specific accomplishments. The vast majority of intelligence resources is contained within the HUMINT, SIGINT, and IMINT programs. The agencies that execute the bulk of these resources are CIA, NSA, NIMA, and

[33] "Making Intelligence Smarter, The Future of U.S. Intelligence", Report of an Independent task force sponsored by the Council on Foreign Relations, Maurice R. Greenberg, Chairman. http://www.copi.com/articles/IntelRpt/crf.html

NRO. Each of these agencies has responsibilities spanning the full spectrum of customers; and NSA and NIMA are additionally designated as DoD Combat Support Agencies. Within the analytic elements of the IC, resources tend to be organized around missions; all-source analysts fuse data from all intelligence disciplines to provide products to their customers, while discipline-specific analysts generally provide a "stove-pipe" perspective.

This situation is not unlike the DoD, where the Services organize, train, and equip, while the combatant commands execute the joint warfighting mission. This task force concluded that the IC's performance would be enhanced if it adopted the broad objectives of the Goldwater-Nichols Act in strengthening the authority of the *joint* community. In particular, we recognized the need to have strong mission-focused components that:

- Are accountable for providing the requisite intelligence to their primary customers;
- Are empowered to drive resource allocation decisions to enable execution of their missions; and
- Are responsible for increasing attention to strategic issues within their Area Of Responsibility (AOR) – effectively balancing those requirements against tactical and operational support.

Recommendation 1. ***The DCI should designate and empower Mission Managers within the Intelligence Community who are accountable to their primary customers for delivery of intelligence on issues involving their Area of Responsibility.***

We noted that while the all-source analytic elements in the CIA, DIA and INR are vested with the responsibility for providing intelligence to their respective primary customers, they have minimal influence on the allocation of intelligence resources. We are not proposing a wholesale reorganization of the IC, but rather a strengthening and empowering of the analytic elements – giving them the expertise and the clout needed to stimulate transformation of our intelligence apparatus. Our analogous model is:

Department of Defense

Services → Organize, train, equip
Geographic CINCs → Warfighting

Intelligence Community

Collectors – "INTs" → Collect, exploit, equip
Mission Managers → ***Deliver intelligence***

In this construct, the Mission Manager is responsible for adjudicating priorities across the spectrum of IC customers – and has significant authority to influence allocation of NFIP resources.

We considered a variety of organizing principles in defining the AORs for Mission Managers, only to conclude that there is no perfectly orthogonal set. Many potential adversaries are inextricably anchored to geography – although related issues of concern frequently span geographic borders. Other threats stem from highly mobile adversaries with minimal geographic ties. We could conceive of no set of AORs that were completely independent from one another. We therefore recommend adoption of AORs that are consistent with those of the DoD Commander-in-Chiefs (CINCs) where applicable, as we believe this would better align and strengthen support to the warfighter – providing the J-2 elements with a stronger voice. The remaining AORs are focused on cross-cutting issues of strategic importance. In particular, while there is no readily identifiable customer for homeland defense, we believe it important to address this emerging issue – and we suggest that an early focus be support of the Joint Task Force for WMD Consequence Management at USACOM. We suggest designation of ***Mission Managers*** for the following AORs:

Mission Manager: Primary Area of Responsibility

• Europe • Pacific • Mid East/Africa • Latin America • Atlantic	• Strategic Threats • Transnational Threats • Homeland Defense • Emerging Issues

We believe each of these AORs warrants enough individual attention to justify a specific owner and advocate.

Mission Managers should be, first and foremost, accountable for delivering intelligence to their primary customers on issues involving their AOR – and their performance should be judged by those customers. The optimal structure would incorporate mutual dependencies. In this strategy, the mission managers are dependent upon the collection, processing, and exploitation capabilities resident within the "INT" stovepipes, while (and this is a change) the "INT" program managers are dependent on the mission managers for a prioritized set of requirements that is in sync with their available resources.

Recommendation 1.1 ***The Deputy Secretary of Defense should ensure that DoD customers of the IC clearly define their intelligence priorities – for strategic, operational, and tactical support – and provide periodic performance evaluations to the accountable Intelligence Mission Managers.***

Under this construct, the J-2 components would represent the CINC's prioritized current and future requirements to the Mission Manager, and would provide an assessment of how effectively those needs were met by the IC. Similarly, other all-source elements of the DIA would prioritize and advocate the needs of additional DoD customers.

We recommend assigning the following suite of responsibilities – together with delegation of the authority commensurate with these responsibilities:

Mission Manager: Primary Roles and Responsibilities

- Deliver timely intelligence to support customer objectives – in the form desired by the customer
- Establish priorities, derived from our national security strategy, to support resource allocation decisions
- Develop and maintain system-level strategic understanding of adversaries
- Drive collection and exploitation via prioritization of tasking
- Develop *measures of effectiveness* against which collection assets are evaluated – to motivate elimination of less productive capabilities and more effective allocation of investment resources
- Employ a robust suite of analytic methodologies including scenario-based approaches and modeling and simulation to yield more robust insights into emerging issues
- Identify new observables and gaps in collection capabilities
- Prioritize strategic investment across the full spectrum of personnel and technology-based capabilities (to enable all phases of the intelligence process)

Successful execution of these responsibilities will require a robust set of skills together with a significant ability to influence resource allocation decisions. The range of expertise in each unit must include substantive knowledge relating to the AOR, analytic skills, and knowledge of collection assets, as well as the requisite leadership, strategic planning, and program management skills.

Under this construct, the intelligence disciplines – "INTs" – retain the responsibility for developing and deploying required discipline-specific capabilities, just as the Services are responsible for equipping future warfighters. Their challenge is to optimize in a different dimension – across the priorities established by the various Mission Managers – knowing that their ability to respond to the unique needs of each AOR will be measured by that Mission Manager.

To be effective, the personnel incentives of the IC must be realigned to motivate successful *mission* execution. Here again, an element of the DoD model is applicable – requiring joint service (that is, service in a mission-focused component) before progressing to the ranks of Senior Intelligence Service (or Senior Executive Service) within the ranks of intelligence professionals. This would provide discipline-focused staff with a greater appreciation for the overall intelligence mission. Note that it is equally important that mission-focused staff have an understanding of the various intelligence disciplines – and would therefore benefit from a similar rotational tour.

ENTERPRISE INTEGRATION

"The new source of power is not money in the hands of a few but information in the hands of many."
John Naisbitt, 1984
Megatrends

When a new age is entered, technology leads by approximately two decades the organizational, policy, strategic, doctrinal, and cultural changes necessary to exploit the new technologies. The limiting factor in progress is rarely our ability to imagine the future, or even to invent it, but most often our willingness to embrace it. The greatest inhibitors to achieving *Decision Superiority* are cultural – the resistance to sharing information. In the 21st century, information will be used as an instrument to preserve the peace and – failing that – as a weapon in war. Information of all descriptions, and the electronic and photonic arteries that carry it, will increasingly become global utilities and commodities. Shared information will no longer be an oxymoron.

Virtually every evaluation of the IC has noted the need for greater collaboration and sharing of information among the individual IC components, more routine engagement of the expertise that exists outside the IC, and robust integration and sharing of information between the IC and the customers it serves. There are three parameters that either enable or inhibit such behaviors:

- Security policy
- Information infrastructure
- Operational processes

In today's IC, all three parameters serve as inhibitors. In a viable 21st century intelligence enterprise, all must be enablers. For this recommendation, we believe that an emerging industry model – that of eBusiness – is appropriate. The chart below contrasts the characteristics of a traditional Industrial Age business with those of an eBusiness.[34]

[34] "eBUSINESS IMPERATIVE", The Concours Group, www.concoursgroup.com.

Issue	Industrial Business	eBusiness
Basis of competition	Products and services	Business models
Barriers to entry	Physical constraints, branding, financial capital	Intellectual capital, brand power
Control	Producer	Customer
Marketing, sales and service	Mass marketing	Mass personalization
Time to market	Development time: fits and starts	Web time: approaching zero
Pricing	Local/account focused	Web-pricing: Global, real-time, individualized, transaction costs approaching zero
Logistics	Receiving, storing, and distributing inputs and products; suppliers, warehouses, inventory, transportation	Building a network of strategic partners for just-in-time processing; instantaneous delivery of information products; industry-wide exchanges
Operations	Physical processes	Added knowledge
Organization	Silo-based departments	Multifunctional, agile teams

Since intelligence is an information-based business, it can be effectively implemented in the eBusiness model. Under this construct, the customer has greater control – coupled with the expectation that needed information will be available in the desired format in near-real-time. It is important to recognize that even if the IC chooses not to adopt this model, its competitors are already doing so. And unless the IC provides timely, value-added intelligence, it runs the risk of being judged irrelevant.

We believe such an enterprise is unlikely to emerge from the current IC assignment of roles and responsibilities, and therefore recommend that the DCI delegate ownership of this important objective – realizing that the initiative demands step-by-step coordination with key customers.

Recommendation 2. ***The DCI should designate and empower an Intelligence Enterprise Architect who would be accountable for definition of IC-wide security policy, information infrastructure standards and protocols, and development of cross-cutting operational processes.***

To be effective, the Intelligence Enterprise Architect must have direct authority over some NFIP resources, significant influence on the allocation of related resources, and the ability to enforce adherence to enterprise standards and policies – while simultaneously ensuring that these standards and policies are in concert with those of key customers.

To implement this new model, IC personnel incentives must be realigned to motivate individuals to collaborate and share information – that is, to create multifunctional, agile teams. We believe that sharpening the focus on intelligence missions – as described in the previous section – will help provide the necessary personnel motivation.

SECURITY POLICY

Primary customers in every segment have expressed the need for more usable intelligence – that is, intelligence designed with customer objectives in mind. Very often, a major issue is the customer's inability to share the intelligence with coalition partners, or to use it for diplomatic purposes, for fear of exposing sensitive sources and methods. The DCI is tasked by Executive Order 12333 to "ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products." But in the same Executive Order, the DCI is also tasked to "ensure that programs are developed which protect intelligence sources, methods and analytical procedures." Today's IC security policy – a legacy of the pre-networked, Cold War world – tilts the scales toward protection of sources and methods and inhibits sharing of intelligence.

The problem is exacerbated by a perception among some data owners – and analysts – that information increases in value in proportion to increasing levels of classification. In this context, the value of Top Secret data is thought to be greater than that of Secret data – and much greater than that of open source information. Even worse, the owner of the highly-valued (i.e. highly-classified) information is seen as more important than the owner of lesser-valued information. This phenomenon results in information hoarding, over-classification, and undue avoidance of open sources – precisely the behaviors that inhibit collaboration and sharing of information.

We are not arguing that protection of sources and methods is unimportant. Indeed, there is ample evidence to suggest that previous exposure has diminished the value of some of our legacy collection capabilities. (Although ironically, the same effort appears to be applied to "protection" of technical collection assets even after they are known to have been widely exposed.) But customers of the IC see no value in the collection of intelligence that is not available for their use – in *their operational context*. We have already described the information-sharing challenges confronted in coalition operations and in supporting the objectives of homeland defense; equivalent challenges exist in supporting diplomatic operations.

This task force believes the IC should take a fresh look at their security policy across the board. We believe that in place of today's collector-centric *need-to-know* security framework, the IC should establish a mission-centric *need-to-share* construct. We acknowledge that there have been some attempts to establish Communities of Interest (COI) around specific missions, but believe success has been limited by the collector-dominated security model currently in effect. We further believe that maturing technologies such as public-key-infrastructures (PKI) offer an opportunity to support effective collaboration and sharing while maintaining protection of truly sensitive data. And, finally, we believe that emerging tools will enable more robust real-time auditing and adaptive security management – providing even stronger protection for sensitive sources and methods.

But basis of the solution lies not in technology, but rather in changing the security culture whose operating model is "system-high" – with need-to-know barriers placed at network perimeters. Personnel incentives must be realigned to motivate collectors and analysts alike to identify the means to appropriately share intelligence – while still maintaining vigilance over sensitive sources and methods. And such solutions must be developed in concert with key customers.

Recommendation 2.1 ***The DoD's Chief Information Officer should partner with the Intelligence Enterprise Architect in the development of a security model that enables effective intelligence support for the coalition warfighting environment.***

INFORMATION INFRASTRUCTURE

The term *Infosphere* has been coined to represent "the fusion of all the world's communications networks, databases, and sources of information into a vast, intertwined, and heterogeneous tapestry of electronic interchange."[35] A ubiquitous global information system assembled from standard, commercially available tools and technologies and continuously nourished by information from myriad sources will be the *digital nervous system* of any successful 21st century enterprise – including intelligence.[36]

Strategies emerging from our U.S. military services embrace the concept of Network-Centric Warfare – using robust information systems to coalesce strategies, operations, and tactics. Major features of this vision include:

- A network of widely dispersed forces with precise situational and positional awareness
- Supported by a synchronized and fully integrated information domain that includes data from both national and organic sensors
- And enabled by powerful correlation engines that fuse all-source information and intelligence

It is an elegantly assembled information system that will enable the warfighter to find, fix, track, target, assess, engage, and destroy the enemy.

The challenge for the IC is twofold: it must create such an integrated information infrastructure to enable its own operations; and it must act as a "feeder" to the warfighter's information domain to support military operations. Both require a robust global information infrastructure built on commercial standards and protocols; and both require that intelligence data, tagged with precise temporal and spatial attributes, be accessible – to customers and IC components alike – via this common infrastructure.

Recommendation 2.2 ***The DoD's Chief Information Officer should partner with the Intelligence Enterprise Architect to ensure the implementation of technology and data architectures and standards that are compatible with the DoD's Integrated Information Infrastructure.***

[35] The Navy and the Infosphere," Michael Vlahos and Dale Pace, Johns Hopkins University, Applied Physics Laboratory, JWR-99-02.

[36] *Business @ The Speed of Thought*, Bill Gates, Warner Books, Inc. Copyright 1999, ISBN: 0-446-52568-5.

Operational Processes

There are two core processes that we believe are critical performance enablers for the 21st century intelligence enterprise:

- Collaboration – enabled by emerging decision support tools
- TPED – the full cycle of tasking, processing, exploitation, and dissemination of intelligence

Both require a foundation of enabling security policy and a robust integrated information infrastructure.

Collaboration – especially distributed collaborative planning – is a powerful performance enabler. Rudimentary tools are already commercially available to support collaboration among geographically dispersed teams. And more sophisticated decision support systems are emerging that will solve complex problems through the exploitation of distributed collaborative computing and the utilization of artificial intelligence methodologies and rule-based systems. Such sophisticated decision support systems will have a profound impact on our current hierarchical command and control structures. And such decision support systems will be key enablers to collaborative processes in the 21st century intelligence enterprise.

Enterprise collaboration must be effectively supported in multiple dimensions:

- Between the IC and its customers – to ensure responsiveness amidst rapidly changing priorities
- Between analysts and colleagues external to the IC – to ensure that the best available talent is routinely brought to bear on intelligence problems
- Between analysts and collectors – to ensure that today's collection assets are effectively deployed and strategic investments are targeted to address gaps
- Between IC developers and external partners – to ensure that commercial advances are fully exploited
- Among collectors – to ensure synergistic allocation of current collection assets and strategic investment resources

To attain the necessary agility for success in the 21st century, this spectrum of collaborations must be effectively supported via the intelligence enterprise information infrastructure.

In concert with its customers, the IC should investigate the development and deployment of applications that parallel the "push technologies" underpinning Internet-delivered news services such as PointCast. These services – already in wide use in both industry and government – would enable the intelligence customer to personalize the information channels (sources and topics) from which information is continuously and instantaneously delivered. In a properly secure environment, this type of support could be integrated with a wide spectrum of context-defining open sources – including newspapers, television, and the Internet. Further, a "click" on a featured topic could enable collaboration with an intelligence analyst via videoconferencing.

Previous studies and reports have highlighted the need for an effective TPED process; this is particularly critical to effective support of the near real-time requirements of the warfighter.

Most of the discussion has focused on IMINT – both as a readily taskable collection asset and as a geospatial reference point against which other intelligence data can be tagged. As a result, a recent DSB report recommended that NIMA be assigned responsibility to develop and deploy a TPED system for IMINT – and subsequently for the IC – while acknowledging that today's NIMA is not appropriately organized or sufficiently skilled to perform this task.

This task force agrees that the IC must develop an enterprise-wide TPED process that is deployed on the intelligence information infrastructure and is readily accessible to primary customers – enabling rapid response to immediate customer needs. But we remain skeptical of NIMA's ability to perform this task and recommend that the Intelligence Enterprise Architect be assigned the TPED responsibility for the IC – with the option of designating NIMA as the Executive Agent.

An important attribute of the intelligence TPED process would be "hands-off" direct tasking of certain collection assets for time-critical, high-priority operations. The overall IC process should, however, be sufficiently robust to permit replacement of today's many collection management committees with a decision support system that enables intelligence Mission Managers to work collaboratively with collectors to ensure effective allocation of the entire suite of collection assets.

The TPED challenge is exacerbated by the fact that an effective system should also drive tasking of organic theater assets – which are outside the control of the IC. We believe the IC's TPED process should be compatible with – or perhaps extensible to – a DoD-developed process for tasking of tactical assets. The DSB Force Modernization task force has devoted significant time and attention to the development of a high-level operational architecture to support joint warfighting operations, and has recommended that the U.S. Joint Forces Command (USJFCOM) be assigned the responsibility for future joint C^4ISR systems architectures and technical capabilities. We therefore recommend that USJFCOM serve as the DoD executive agent responsible for ensuring that a unified TPED process is developed that drives both theater and national intelligence assets.

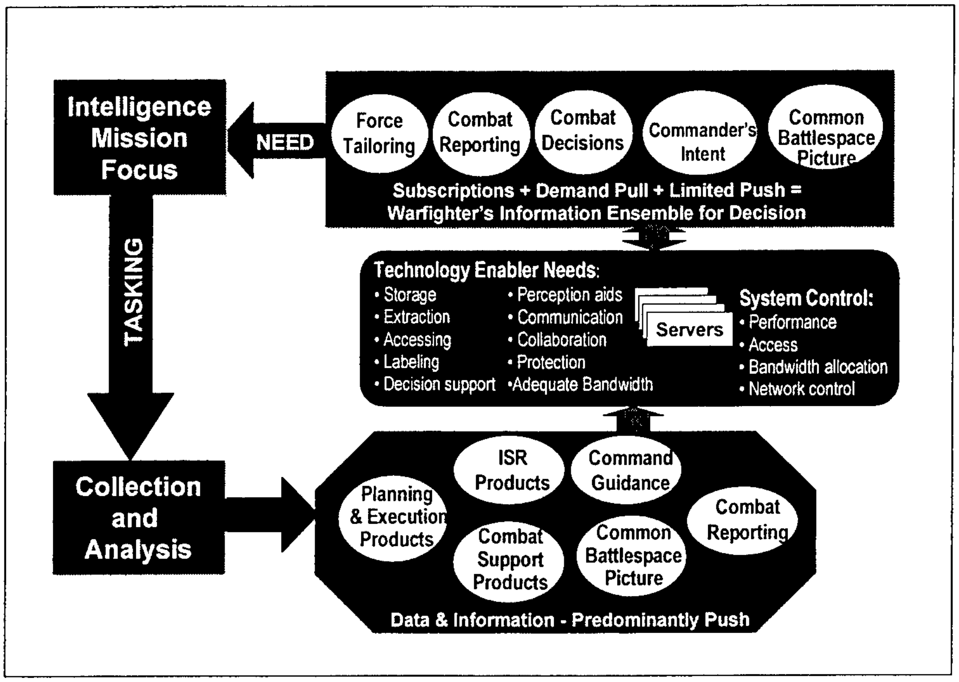
Recommendation 2.3 ***The Deputy Secretary of Defense should designate USJFCOM as the DoD executive agent for TPED – and task them to develop an integrated process for the tactical and theater assets and ensure interoperability with the IC's TPED process.***

IC Support to the Warfighter's Information Ensemble

Effective support of the IC's warfighter customers will require that the intelligence information infrastructure – and operational processes – interface with the DoD's operating environment. This is at present a formidable challenge as the Services have individually developed information infrastructures and the *joint* operating environment is not yet clearly defined.

Enablers for the DoD's joint operating environment span the spectrum from coherent security policy to an interoperable technological infrastructure to integrated operational processes – the same attributes identified as critically important for the 21st century intelligence enterprise.

In this year's DSB Summer Study, the following high-level operational architecture is used to describe the necessary interaction between the IC and its DoD warfighter customers:



It is critically important that the IC and the DoD work in concert to achieve this vision.

CONTINUOUS TRANSFORMATION

"Yet if times stay tough and the New World Order evolves without any new big-power confrontations, the need for innovative, rapidly developed, and relatively inexpensive systems that are best supplied by a Skunk Works will be greater than ever."

Skunk Works[37]

As long as our adversaries followed fairly predictable tactics in a slowly changing national security environment, our conventional approach to creating and introducing new intelligence capabilities was adequate. But with the present high operational tempo and a complex environment where our adversaries are dynamically adapting their own capabilities – and routinely using unexpected methods to deny and defeat our previously successful capabilities – greater agility is required within our intelligence enterprise.

One method of introducing new technologies into established operations that has proven to be successful is generally called the "skunk works" approach. This term emerged from the Lockheed Skunk Works, but for a much longer time the experimental or Darwinian approach to advances has been shown to be very effective by successful visionary companies. In *Built to Last,* the innovative practices of such companies as Johnson & Johnson and 3M are described.[38] The basic idea used by 3M is to "*try a lot of stuff and keep what works.*" The barrier to this approach in a highly regulated bureaucratic environment is the tyranny of requirements, namely that *if it is not prescribed, then it is not permitted.*

The top-down requirement and regulation-driven approach has valuable political benefits for a bureaucracy that is continually scrutinized for someone to blame when things go wrong. No one in a bureaucracy with any memory capability or who has suffered the blame and scandal that too often results from a reasonable mistake, will be ready to rush out and try risky experiments again. Indeed, the requirements process with well-defined milestones often demands success – and such legislated success can be the ultimate cause of failure.

On the other hand, the rules followed by 3M are a proven way to achieve a creative environment that leads to continuous introduction of new products that compete well in the marketplace. Some of the 3M tenets that have been used over the years are as follows:

- "If you put fences around people you get sheep."
- "Hire good people and leave them alone."
- "Encourage experimental doodling."
- "Give it a try – and quick!"

[37] *Skunk Works,* Ben R. Rich & Leo Janos, Little, Brown and Company. Copyright 1994, ISBN 0-316-74330-5.

[38] *Built to Last, Successful Habits of Visionary Companies,* James C. Collins & Jerry I. Porras, HarperBusiness. Copyright 1994, ISBN 0-88730-671-3.

We acknowledge that 3M has, in many respects, a much easier task – after all, their corporate livelihood depends on innovation and the metrics indicating success are clear. Even so, we believe there are lessons to be learned from their model that apply to our intelligence apparatus. In fact, we would argue that continuous innovation is equally critical for a successful 21st century intelligence enterprise.

Within the DoD, the Advanced Concept Technology Demonstration process was "initiated to permit the early and inexpensive evaluation of mature advanced technology to meet the needs of the warfighter."[39] ACTD selection criteria include:

- Timeframe for completing the evaluation of military utility is typically two to four years
- The technology should be sufficiently mature
- The ACTD provides a potentially effective response to the military need
- Users sign up to be intimately involved in the ACTD
- A lead service/agency has been designated
- The risks have been identified, understood, and accepted
- Demonstrations or exercises have been identified that will provide an adequate basis for the utility assessment
- Funding is sufficient to complete the planned assessment of utility and to provide technical support for the first years of fielding of the interim capability
- The developer is ready to prepare a plan that covers all essential aspects

This process shares some of the high-level objectives of the skunk works approach, but its success – in terms of new operational capabilities for the warfighter – has been mixed. Nevertheless, we would once again argue that there are valuable lessons that, if applied, would help create the needed 21st century intelligence enterprise.

Recognizing the importance – and the difficulty – of transforming the capabilities of our military, the DoD recently established experimentation as a new military mission.[40] Their fundamental objective is the *acquisition of knowledge to guide decisions about an uncertain future*. By designating USJFCOM as the Executive Agent for Joint Warfighting Experimentation, the DoD has established an institutional home for the process in the *joint* – that is, the mission-focused warfighter – community rather than vesting the responsibility with each of the individual Services.

Within today's IC, we found no mechanism to support continuous transformation of the apparatus – that is, the changing of the processes, tools, and talents to more effectively execute intelligence missions in a dramatically changed, and continually changing, global environment. While pockets of innovative work certainly exist, they are the exception rather than the rule; and they are often sacrificed to operational pressures and maintenance of legacy systems. Furthermore, the scale of most such efforts will at best have discipline-specific – rather than enterprise-wide – impact.

[39] "ACTD Questions and Answers," http://www.acq.osd.mil/at/question.htm

[40] Department of Defense News Release 252-98, "U.S. Atlantic Command Designated Executive Agent for Joint Warfighting Experimentation," May 21, 1998.

Recommendation 3. ***The IC should establish and institutionalize a program – and an environment – to foster innovation and enable continuous transformation of enterprise-wide capabilities to yield sustained success against the dynamic global environment.***

A variety of organizational approaches to creating an environment of continuous transformation – some of which have been previously described – exist within industry and government organizations. Rather than prescribing a solution, this report sketches the broad outline of a potential model together with what we believe are the necessary preconditions. Our approach has been variously referred to as a *skunk works* and as an *amoeba* – the intent is to continually create small units that embody needed new capabilities, and to enable these units to replicate, or scale, into operational capabilities.

It is important to note that this recommendation is more likely to succeed if the top-level recommendations of previous sections of this report are implemented. That is, enterprise-wide problems to be tackled by these units should be identified and prioritized from an intelligence mission perspective, i.e. by *Mission Managers.* And experiments should be crafted such that successful new capabilities can be integrated into the overall intelligence enterprise, i.e. designed in concert with the *Intelligence Enterprise Architect.*

ENABLING CONTINUOUS TRANSFORMATION

There are several prerequisites to be satisfied before initiating an enterprise-wide program of innovation and experimentation – especially in today's resource-constrained environment. Key success factors include:

- Sustained high-level commitment (DCI and Deputy Secretary of Defense) to set aside and protect program resources
- Support for well-managed, high-risk experiments, realizing that experiments fail only if there are no lessons learned
- Strong mission pull to identify important problems
- Prioritization in collaboration with primary customers
- End-to-end systems approach to every problem
- Engagement by end-users throughout the experiment to ensure the utility of emerging solutions
- Visionary leadership of every project
- Commitment to engage the best talent and most viable technologies whether from government, industry, or academia

While acknowledging the challenges inherent in each of these statements, we believe the ultimate objective – an agile intelligence enterprise that continually self-optimizes against the dynamic global environment – is a vital component of our 21st century national security establishment and therefore warrants this commitment. And we are convinced that the IC strategies in place today will not attain this goal.

In our lexicon, we use the term *program* to mean the overall institutional umbrella and the resources devoted to this effort. The program, which could be managed by a small Transformation Program Office (TPO), is comprised of a dynamic portfolio of projects – each with its own project manager and project team. These project teams are temporary; they exist only for the duration of the project – typically 2-5 years. Team members are selected to bring a spectrum of talents and capabilities matching the problem at hand. Selection to these project teams must be viewed as a career growth opportunity – and rewarded as such – to motivate top talent to participate. In general, project teams should include both intelligence professionals and talent drawn from outside the enterprise.

A variety of potential projects are readily identified – spanning the spectrum from problems requiring innovative technology-based solutions to those that are more process or policy-dominated. Illustrative examples include:

- Support to Military Operations
  - Time-urgent precision strike
  - Force protection for expeditionary operations
  - Security framework for coalition operations
- Indications and Warning
  - Strategic attack on the defense information infrastructure
  - Strategic surprise from asymmetric threats
- Homeland Defense
  - WMD early warning system
  - Security framework for intelligence sharing

We make no claim that this is the "right" initial problem set, and believe the IC should invite nominations from throughout the enterprise in addition to targeting major deficiencies flagged in recent reports and assessments. Problems should be prioritized according to mission needs – as established by *Mission Managers* and the *Intelligence Enterprise Architect.*

We recommend a build-up of program resources and project portfolios over a five-year period, beginning immediately. By the fifth year, a resource commitment – based on a percentage of the total intelligence budget (NFIP + JMIP + TIARA) should be established and maintained for subsequent years. Creation of this program as a percentage of the total intelligence effort – regardless of annual budgetary fluctuations – establishes a sustained commitment to continuous transformation of the Intelligence Enterprise, enabling it to adapt to the continually changing external environment. We recommend a starting point of one percent of the total intelligence budget in the first year, adding one percent each subsequent year to reach a total of five percent. We further suggest that some fraction of the program funds be reserved for "new starts" each year – enabling more rapid response to changing conditions.

This investment at the enterprise level does not diminish the need for discipline-specific innovation and experimentation. In fact, it will be important to leverage those local advances into the new enterprise capabilities. There are two basic motivators for establishing this program:

- Synergy – enterprise performance that is greater than the sum of individual contributions from the various intelligence disciplines
- Seams – new capabilities that might never emerge from today's stovepipes because of their multi-disciplinary character

DoD Linkage

The task force noted earlier that USACOM has been charged to lead the DoD efforts in joint warfighting experimentation. We believe the Intelligence Enterprise's Transformation Program Office should work in concert with USACOM to construct projects of mutual benefit. In particular we would recommend that, at a minimum, the ratio of TPO resources that stem from the TIARA and JMIP budgets be devoted to such activities – and that an early transformation focus should be creation of an integrated TPED process that drives the entire suite of tactical and national intelligence, surveillance, and reconnaissance (ISR) assets.

Recommendation 3.1 ***USJFCOM should ensure that experiments are conducted that fully engage the Intelligence Enterprise and advance our full complement of ISR capabilities.***

In addition, the DoD's ACTD program routinely sponsors projects that have potential benefits or implications for our Intelligence Enterprise. We believe more active partnering at the enterprise level would be beneficial to both sides.

Recommendation 3.2 ***DUSD(A&T) should work with the TPO to construct and sponsor ACTDs that fully engage the Intelligence Enterprise.***

Sustaining Continuous Transformation

History is replete with examples of organizations that were highly innovative and agile when young and small, but lost those attributes as they grew and matured. It could be argued that the NRO – which is not alone, to be sure – provides such an example within today's IC. We therefore believe it important to guard against such an outcome for an organization charged with driving the continuous transformation of the Intelligence Enterprise. Although the Transformation Program was crafted with an eye toward supporting creativity and innovation, history is not on our side so it is worth a brief discussion of likely impediments.

First and foremost, the focus of the program must be on results – enhancing the ability of the Intelligence Enterprise to support its primary customers. And, where feasible, a spiral development approach should be employed to achieve intermediate benefits and maintain customer engagement throughout the project. Losing this focus will diminish support and ensure that new capabilities are never fully operationalized.

Equally important is the caliber of leadership within the Transformation Program Office. This office should be staffed by a small group of visionary, high-energy, highly motivated intelligence professionals. These should be "plum" assignments – highly sought after by the very best talent resident in the Intelligence Enterprise – a true career growth opportunity. If the program is unable to attract this level of talent, failure is inevitable.

Effective staffing of individual project teams is also important. There must be a willingness to engage the best talent – whether internal or external to the Intelligence Enterprise – for the problem at hand. And once again, working on a project team should be viewed as a "plum" assignment. In any case, personnel incentives must be aligned to motivate participation. And the "system" must ensure that the individuals are smoothly transitioned back into their parent organizations upon completion of the project. The goal is to protect the individuals – and exploit the *results* of the team – not to sustain the team beyond the term of the project.

We envision a combination of demonstration and experimentation – believing that a focus on only demonstration will diminish innovation. This means the management processes must be sufficiently flexible to nurture such an environment. Key attributes include the ability to rapidly engage requisite talent, performance-based partnering with external entities (versus specifications-based contracting), and support for prudent risk-taking. It is critically important that project teams have direct authority over the resources required to execute their plan. This process is unlikely to succeed if their time is consumed in *persuading* other enterprise elements to commit resources. That said, establishing tentacles that more broadly engage stakeholders during the project is an important success factor.

As project execution comes to an end, there must be a clear decision regarding transition of the results into full-scale operations. If it is determined that such a transition is necessary, an owner – preferably within an existing component of the Intelligence Enterprise – must be designated. Absence of either of these actions will significantly diminish the likelihood that the potential impact of the project will be fully realized.

We recognize that these precepts are an anathema to many of today's processes, but believe the basics tenet must be:

- Select the right talent
- Trust and empower them to do the right job – and to do the job right

STRATEGIC INVESTMENT

"Nothing is more dangerous than an idea when it is the only one you have."
Emile Chartier, quoted by Roger von Oech
A Whack on the Side of the Head, 1983

In Webster's Dictionary, *investment* is defined as the "outlay of money usually for income or profit," and *strategic* is defined as being of "great importance within an integrated whole or to a planned effect." In our lexicon, strategic investment implies the allocation of today's resources to build discrete skills and technologies that will enhance future performance of the Intelligence Enterprise.

Once again, we believe it vitally important to build and sustain a Strategic Investment Program at the enterprise level. We distinguish this program from the Transformation Program in two dimensions: timeline and life-cycle integration. Beyond that, however, there are significant similarities in our recommended approach – particularly with regard to the need to focus the program against current and anticipated customer needs.

Recommendation 4. ***The DCI should build and sustain a Strategic Investment Program focused on priorities derived from existing – and anticipated – customer needs.***

We recommend a two-pronged strategy – investing in both critical skills and key technologies. We once again recommend a portfolio approach, where individual projects are built around discrete problems. In this instance, however, some of the projects may have significantly longer duration, and execution is likely to be highly distributed. We would not suggest that this investment program replace the discipline-specific investments made by enterprise components, but rather provide an umbrella strategy for skills and technologies with enterprise-wide impact.

STRATEGIC TECHNOLOGY INVESTMENT

Both DoD and DOE have in recent years adopted a "grand challenge" approach to some portion of their technology investment portfolio. We believe the Intelligence Enterprise should adopt a similar approach. Doing so focuses investment strategy against important problems – the solution of which would have revolutionary impact on enterprise performance – and is an effort to guard against the natural tendency of researchers to focus on technological advances rather than results.

A description of such an approach is provided in the "Defense Technology Strategy and Management" section of this Summer Study. In fact, one of their suggested grand challenge themes is equally relevant to the Intelligence Enterprise – *No Place to Hide* – that is, the ability to deny the adversary the ability to hide from our sensors. Tackling such a grand challenge would, for example, result in development of new technologies for close-in, covert, and unwarned collection.

Because there is significant overlap in both the problem set and the technological drivers between the IC and the DoD, we believe that the major investment programs should be well-coordinated. We recognize that there are efforts underway to do just this, but believe the absence of integrated program strategies within either side has limited progress.

Recommendation 4.1 ***The USD(A&T) should ensure that the DoD's technology investment portfolio is coordinated with the Intelligence Enterprise portfolio.***

It is important to note that while the specific technology investments may overlap, the definition of the grand challenge should be context-specific. That is, a military "grand-challenge" is distinct from an Intelligence Enterprise grand challenge – but both may share specific technology investments. An example of this is in the *Bioshield* concept (described in the "Defense Technology Strategy and Management" section) – the challenge of protecting warfighters against biological threats. While many of the same technologies are applicable, the grand challenge for intelligence is to warn of impending attacks rather than to defend or manage the consequences.

Grand challenge themes for the Intelligence Enterprise must be derived from mission needs and developed in concert with *Mission Managers* and the *Intelligence Enterprise Architect*. As the Transformation Program matures, additional themes are likely to emerge from project teams as they tackle increasingly intractable problems. We suggest consideration of the following themes as early organizing principles:

- Master the Infosphere
  - Context-sensitive text search and retrieval; dynamic virtual databases; data fusion; information presentation – beyond visualization
- Template the Adversary
  - Modeling of cultural/sociological parameters; self-updating databases; characterization of operations conducted in subterranean facilities
- Anyone, Anytime, Anywhere
  - Secure, undetectable global communications; covert sensors – and emplacement mechanisms

We recommend centralized management of the technology investment portfolio, with decentralized execution – conducted both internal and external to the Intelligence Enterprise. In such a management construct there must be clearly established objectives, aligned with the grand challenge themes, and measurable intermediate results, as well as a willingness to terminate investment in one technology in favor of another if it appears more likely to yield results. We believe the size of such an enterprise-wide technology investment program should be on the order of 3 to 5 percent of the total intelligence budget (NFIP + JMIP + TIARA), recognizing that additional strategic investments will be made within individual enterprise components.

Strategic Skills Investment

The long-term success of any information-based organization is dependent upon its intellectual assets. Every report, assessment, and study regarding the IC during recent years has identified skilled personnel as a major deficiency. This is not to say that today's intelligence professionals are without talent, but rather that there is not a sufficient quantity of the *right* skills to effectively accomplish the intelligence mission. While individual component organizations are working the skills issue, we believe it is of sufficient importance to elevate it to an enterprise-level issue for critical cross-cutting skills.

It is understandable how the problem came about – and by no means is it unique to the IC. Congressionally mandated downsizing, initiated just when the world of information technology exploded, drove organizations to reduce their workforces through attrition, severely limiting the infusion of new talent. And constrained budgets coupled with increasing operations tempo further diminished investment in workforce training and education. Frankly, as evidenced by the failure of some businesses to adapt to a dramatically altered operating environment, the IC would have been hard-pressed to effect the necessary skills transformation even under the best of circumstances.

A successful 21st century Intelligence Enterprise needs a robust strategy for building and sustaining skills critical to its performance – augmented by a strategy to engage and leverage relevant talent external to the enterprise. Components of such a strategy will include:

- Identification of critical skills – and active nurturing of the individuals who embody them
- Targeted hiring to increase the internal talent pool
- Identification of external pools of talent – and creation of long-term alliances

Strategy components must be robust against changing workforce demographics and motivations. Thus, additional strategic considerations will include flexibility in compensation and benefits packages – and acceptance of the reality that a smaller percentage will contemplate "lifetime" employment in the IC.

Once again, we believe the identification of critical skills should derive from intelligence mission needs, but there are two broad categories that have been repeatedly identified that should be at the top of the list for sustained strategic investment:

- Science & Technology
- Intelligence Analysts

Both of these skills sets are distributed throughout the enterprise, and each has specific challenges to overcome in strengthening the enterprise workforce.

Many of the challenges in building a strong science and technology workforce within the Intelligence Enterprise are immediately apparent: inability to compete with commercial industry compensation; high ratio of foreign nationals with appropriate skills; increasing tendency toward frequent job changes; and perceived lack of opportunity to keep skills current within the government environment. On the other hand, the Intelligence Enterprise can offer tremendously exciting, challenging, and rewarding work – if it creates the environment to do so. The Intelligence Enterprise can also devise more robust training and education programs to overcome the perception that the insularity due to security restrictions will result in the deterioration of an individual's skills. Even so, we believe the Intelligence Enterprise must develop strategies to deal with the remaining challenges that currently impede its ability to attract and retain a strong science and technology workforce.

Analysis is one of the core competencies of today's IC, but it must be significantly strengthened in several dimensions. The evolving threat environment, briefly described in section IV, contains a greater diversity of potential adversaries – each with distinct culture, language, and moral codes. The skills necessary to analyze these threats are, in general, not fungible. This is not a new observation, but it is one that poses significant challenges for a 21st century Intelligence Enterprise. There are programs underway within today's IC to build analytic depth in specific areas – using such approaches as overseas rotational assignments. While these programs are an excellent first step, they are not currently of sufficient size or scope to have the enterprise-wide impact that is needed. And while such issue-specific analytic depth is essential, equally important are the analysts who understand the growing global interdependencies – driven in part by the technology environment. Development of such broad-based expertise and intuition will require a different type of investment strategy. Additionally, intelligence analysts must increasingly master the technology-enabled global information environment – including the ability to work with the science and technology workforce to create useful new enabling tools. Each dimension is of such importance that it should drive explicit enterprise investment strategies.

It should be noted that the need for knowledge of cultures, languages, and moral codes is equally important for case officers, as is the need for them to make better use of technology-based tools. While these training programs share many common elements, we believe they are best managed at the organization level rather than as enterprise-wide activities.

MAKING IT HAPPEN

"The only things that evolve by themselves in an organization are disorder, friction, and malperformance."

Peter F. Drucker, 1976
Wharton Magazine

The recommendations in the preceding chapters are designed to build from one to the next rather than being a set of independent actions. This not to suggest that each recommendation in isolation from the others is without value, but rather that the cumulative impact would be greater. This section, therefore, provides a potential integrating framework for the individual recommendations. Our goal is to purposefully create a 21st century Intelligence Enterprise with the following attributes:

- Robust against widely diverse issues, while maintaining sufficient depth on each to enable precision operations
- Agile amidst rapidly changing priorities, while maintaining vigilance over important strategic issues
- Anticipatory – able to predict and deal with the important changes in global conditions
- Fully integrated with the customer communities it serves

The matrix below correlates these attributes to our four primary recommendations.

	Mission Management	**Enterprise Integration**	**Continuous Transformation**	**Strategic Investment**
Diversity of Issues			X	X
Depth & Precision		X		X
Agility	X	X	X	X
Strategic Focus			X	X
Anticipatory		X	X	X
Customer Integration	X	X	X	X

Earlier in this report we observed that the DCI has three distinct roles:

- President's Intelligence Advisor
- Leader of the Intelligence Community
- Director of the Central Intelligence Agency

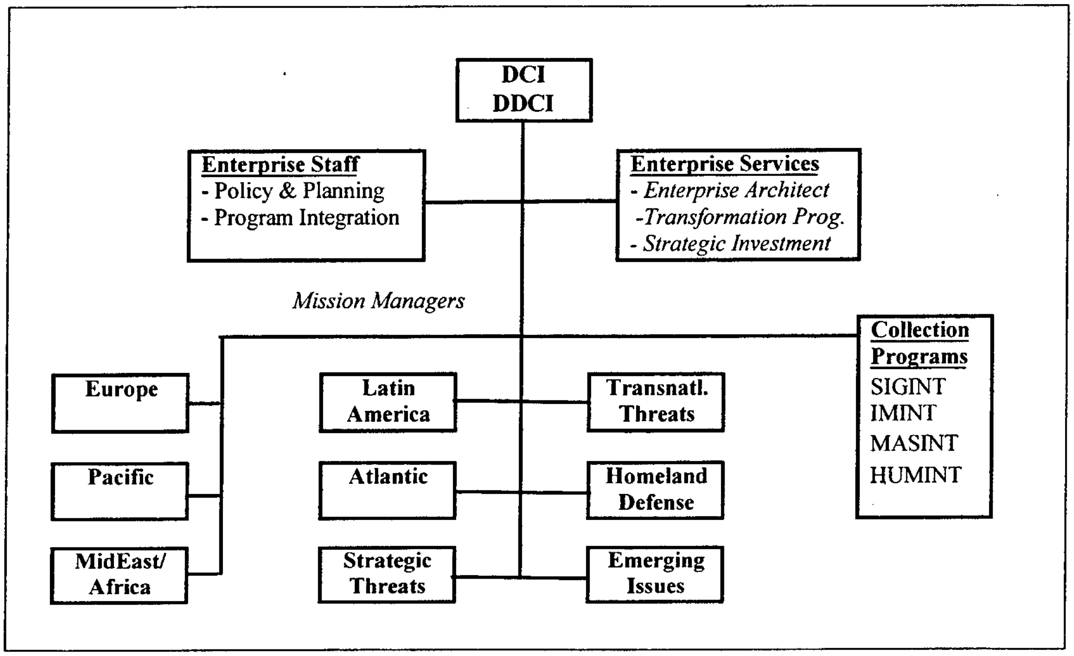
Each role is a formidable task, and the combination of the three would be an overwhelming challenge even during a period of relative stability. But the foreseeable future is anything but stable, and we believe that it is time to revisit – and modify – this assignment of roles. Previous reports have also considered this topic; their recommendations have ranged from status quo to dramatic restructuring of the community.

We believe the roles of President's Intelligence Advisor and leader of the national intelligence effort are – and should remain – inextricably linked. We further believe that to effectively execute these related responsibilities, the DCI must have direct chain-of-command authority over the *Mission Managers* and their organizations – the mission execution elements of the 21st century Intelligence Enterprise. And that leadership of the Intelligence Enterprise from a mission perspective would enhance its overall performance and strategic posture.

In specific terms, this separates the two core functions of the CIA – all-source analysis and clandestine human collection – with the all-source analysts becoming the core of the Mission Management Units. Under this model, the CIA's Directorate of Operations would form the core of a separate organizational entity – still reporting to the DCI, but not on a daily operational basis. We would recommend that this new organizational entity be designated as the Clandestine Collection Organization (or Agency), integrating the relevant components from the CIA's Directorate of Science and Technology and possibly other related activities.

We realize this proposal is highly controversial and potentially impossible to implement, but believe it would significantly enhance the DCI's ability to provide the needed leadership for the Intelligence Enterprise – both as perceived by other components and in reality by enabling focus on mission execution rather than discipline-specific issues.

The organizational construct below provides the broad framework for our recommendations. We have made no attempt to include all elements of today's IC but instead have shown how our recommendations would shape the core structure of the Intelligence Enterprise.



This proposed construct leaves many questions unanswered. For example, the SIGINT, IMINT, and MASINT programs are today managed by DoD components and therefore have established line organization reporting relationships. The HUMINT program is, however, today managed by the CIA, an independent agency. Separation of this program from the core of the Intelligence Enterprise would require that a new reporting relationship be established. Ideally, we would recommend creation of a new agency for Clandestine Collection that would fall under the umbrella of the Intelligence Enterprise but would have its own Director. The objective is to enable the DCI to focus his attention on the dual roles of President's Intelligence Advisor and Director of the Intelligence Enterprise.

Also undefined are the precise relationships between the Enterprise Mission Management Units and the department-specific analytic units (e.g. DIA, INR). The proposed construct is not intended to usurp the responsibilities of these elements, but rather to strengthen their voice in the resource allocation process. More robust collaboration and sharing of information and analytic results across this broader analytic community – enabled by the integrated infrastructure – would be expected.

We would expect the Community Management Staff to morph into the Enterprise Staff, but at the same time become more robust – taking on a role akin to the Joint Chiefs of Staff. The Enterprise Services organization could be modeled after USJFCOM as it fulfills its roles as the joint forces command. Finally, we believe personnel incentives must be aligned to motivate service in the core Intelligence Enterprise organizations – much as *joint* tours are a prerequisite to promotion in the military. While we would caution against precise mapping of the DoD construct and processes, we provide the analogies here for illustrative purposes.

We acknowledge the difficulty of effecting the organizational and cultural changes that we propose in this report, but believe continued incremental adaptation will have marginal impact – and will be insufficient to cope with the demands of the 21st century. In short, we agree with the opinion expressed by Admiral William Owens, USN (Ret.), who argued that the rate at which the transformation of our U.S. military will proceed "***depends greatly on what the Intelligence Community does and does not do over the next several years; what it becomes or refuses to become; whether it leads or retards the transformation***."[41]

[41] American Intelligence Journal, "Intelligence in the 21st Century," Admiral William A. Owens, USN (Ret.), AIJ 1999, Volume 19, Nos. 1&2, ISSN 0883-072X, pp15-21.

ANNEX A. MEMBERSHIP

Co-Chairs:	Dr. Ruth David, ANSER
	Lieutenant General Ken Minihan, USAF (Ret.)
Members:	Mr. Brian Cullen, Consultant
	Mr. Charles Hawkins, Consultant
	Dr. Edward McMahon, MRJ Technology Solutions
	Mr. Frank Marchilena, Raytheon
	Mr. Peter Marino, Firearms Training Systems, Inc.
	Major General Rich O'Lear, USAF (Ret), Lockheed Martin
	VADM Jerry Tuttle, USN (Ret), MANTECH Systems Engineering Corp.
	Dr. Paul Weiss, Penn State University
	LTG James Williams, USA (Ret), Consultant
	Dr. Gerry Yonas, Sandia National Laboratory
Exec Secretary:	Mr. Bruce Brody, OASD (C3I)
Government Advisors:	Mr. Luis Acosta, Joint Staff, J-8
	MAJ Jerry Blixt, USA, Joint Staff, J-2
	Mr. Robert Boyd, Air Force Intelligence Agency
	CAPT J. Katharine Burton, USN, DIAP
	Ms. Regina Genton, CIA
	Mr. Harry Lesser, Joint Staff, J-8
	Maj Ed Loxterkamp, USAF, HQ USAF/XOIRN
	Maj Gen Frank Moore, Defense Threat Reduction Agency
	Mr. Patrick Neary, ODCSINT/DAMI-FI
	Mr. David Osias, DIA/DP
	Maj Michael Parkyn, USMC, MCCDC
DSB Secretariet:	CDR Brian Hughes, USN, DSB
Support:	Mr. Christopher Szara, SAIC

PART II. INFORMATION SUPERIORITY

WHAT IS INFORMATION SUPERIORITY

DEFINITION

Joint Vision 2010 defines information superiority as:[1]

> *"The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."*[2]

Information superiority is made up of the full suite of command, control, communications, and computers and intelligence, surveillance, and reconnaissance (C^4ISR) systems as well as information warfare and command and control (C^2) warfare. These pieces provide the information operations, relevant information, and information systems that are the key enablers to the *Joint Vision 2010* construct.

The *Joint Vision 2010* definition for information superiority does not, however, provide a metric for deciding how much information is necessary to successfully prosecute the mission. For example, if information superiority refers only to the adversary, as implied by the term superiority, then the concept can be illustrated, as in Figure 1, where the much higher bar for the United States appears to depict a substantial advantage.

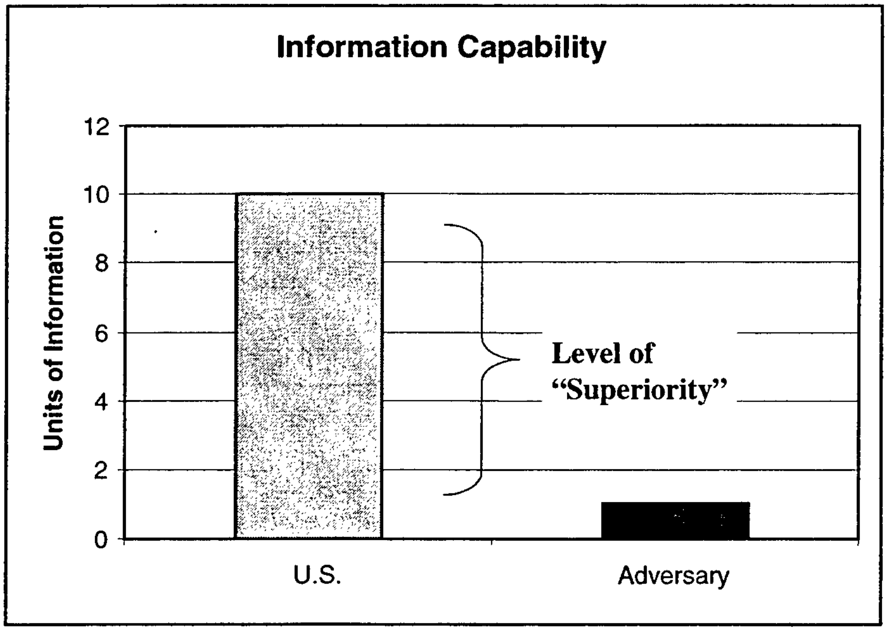


Figure 1: Indication of U.S. Information Superiority

[1] "Joint Vision 2010," July 1996, p. 16.

[2] "Concept for Future Joint Operations: Expanding Joint Vision 2010," May 1997.

Relating information superiority only to an adversary does not, however, explain the difficulty the United States and NATO allies experienced in the recent Kosovo engagement. During those operations, the United States maintained a substantial information advantage over Serbia. Yet the successful prosecution of the mission appeared hampered in several respects: the ability of the Serbian forces to operate within NATO's observe, orient, decide, act (OODA) loop and the ability of the Serbian forces to successfully hide and protect their tactical field forces from NATO bombing.

This experience raises the question of whether information superiority as defined relative to the adversary is adequate. Instead, a different threshold of information appears to be needed – one based upon the rules of engagement used and other external constraints such as the unwillingness to accept any U.S. or allied casualties. Additional constraints, such as weapons and tactics, impose a further increase in the required information. Thus the information required for the United States to successfully prosecute a mission can be much greater than the information needed by the adversary. This concept is demonstrated in Figure 2. As illustrated, the United States may have tremendous superiority over the adversary in information, yet still not meet the level required to execute the mission. The adversary operating with a different objective and rules may be able to counter the U.S. initiative with far less information at its disposal.

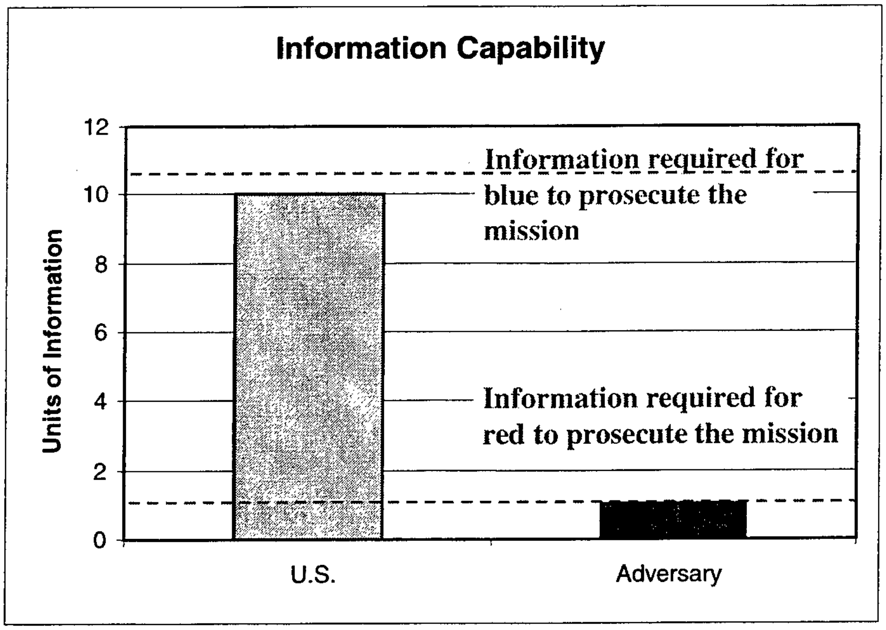


Figure 2: Information Needed to Prosecute the Mission

A better approach – and one taken by this task force – would be to define the attributes of information superiority as:

1. *Information known by one can be known by all.* The knowledge of an area of interest is accessible by anyone with the legitimate need to know, regardless of the geographic location of the inquirer or echelon of the force. This implies complete connectivity across the battlespace as well as a database organized in a readily searchable fashion – organized by spatial and temporal coordinates, for example.

2. *All information comes with a user-accessible pedigree.* To assess the reliability and timeliness of the information, it is critical that the inquirer be able to understand the origin of the data. Data accuracy and assumptions used in interpreting the data need to be available to all the potential users.

3. *The blue OODA loop must be shorter than the red reaction time.* The goal is to provide blue the information and tools to very rapidly decide a course of action. Enhanced decision tools allow for exploring multiple options and potentially gathering additional data to enhance the decision. It is not necessary, nor desirable, to have the blue OODA loop so short that multiple blue actions are executed prior to the first red response. This nonlinear feedback can be counterproductive and produce unnecessary destruction for a specified aim.

4. *Recognition of the fog of war.* It is necessary to know what is unknown. Areas of incomplete or highly uncertain knowledge should be highlighted. For example, unknown conditions due to terrain obscuration should be highlighted as such and not as indications of enemy inactivity. This allows for more prudent course-of-action analysis as well as more efficient tasking and emplacement of intelligence, surveillance, and reconnaissance (ISR) assets.

5. *The capability must be protected and assured.* The information will only be useful if it can be trusted and kept from the adversary. Means for intrusion detection and modification of the information must be put in place. Sufficient security to prevent unauthorized disclosure is critical and must be structured so as not to inhibit transfer to all authorized personnel.

6. *User defined "filter" with defaults.* Information superiority will only be achieved when the end user is able to obtain and assimilate the information quickly and effectively. As a general rule, the user must be responsible for pulling needed information by subscription or by direct request. Since each individual absorbs information differently, and at different rates, the system must be capable of tailoring the information flow to each user. With an increased flow of information, the human-computer interface must be enhanced.

The six attributes defined above form the basis for the discussion in the remainder of this report. Each of these attributes implies a level of sensing, connectivity, database management, and data exploitation that greatly exceeds the current capabilities. To achieve the level of information dominance needed to ensure successful prosecution of future missions requires significant investment by DoD.

MOTIVATIONS

Recent experiences in Desert Storm, Bosnia, and Kosovo point to some new challenges for the U.S. military. A number of current force multipliers for today's force are eroding including military force structure, basing, and control of low-altitude battlespace. At the same time, future adversaries are expected to have much improved access to space, sensing, communications, navigation, and computing.

Even though the United States enjoys unchallenged air-to-air superiority, the emphasis on air combat and restrictive rules of engagement have led recent adversaries to employ new tactics. Surface-to-missiles (SAMs) are used to deny the U.S. airspace; camouflage, cover, and deception (CC&D) are used to hide ground forces and hinder targeting; underground facilities have been employed for hiding critical infrastructure and weapons of mass destruction; and information warfare is being conducted using commercial products and technologies.

The military dominance demanded by the national leadership will require full exploitation of information technology and information operations to realize the goals of *Joint Vision 2010.*

The Information Superiority task force was charged to focus on the need for and use of all forms of information for the United States and coalition partners to achieve full spectrum dominance as required in *Joint Vision 2010.* To address these new challenges the task force examined battlespace superiority issues including:

- U.S. intelligence, surveillance, and reconnaissance (ISR) programs and countermeasures to U.S. ISR systems
- Defensive information warfare operations
- Command and control of 21st century forces
- Detection, combat identification, tracking and targeting of tactical targets obscured by foliage or other cover, concealment, and deception methods

The task force also reviewed the Integrated Information Infrastructure (III) initially described in the 1998 DSB Summer Study and offered recommendations to expand and further its development. To conduct its examination the task force met with representatives from the military Services' information organizations, the intelligence community, Defense Agencies, and civilian information technology community. The task force formed subgroups to look at a variety of specific issues, including continuous reconnaissance, surveillance, and target acquisition (RSTA); R&D and acquisition strategy; Integrated Information Infrastructure; tasking, processing, exploitation, and dissemination (TPED); information operations and protection; logistics; counter-ISR and commercial off-the-shelf (COTS) war; and frequency allocation.

Three major information superiority themes emerged during the study:

- Future adversaries must have ***No Place to Run and No Where to Hide.*** The United States needs to develop new sensors and sensing strategies that are more difficult to avoid. These capabilities include continuous (or near-continuous), on-demand, surveillance; close-in, covert, and unmanned collection; improved, dynamic, information exploitation; flexible targeting; and counter ISR and COTS war. Each of these subjects is discussed in detail in this volume.

- The need for a ***secure Information Infrastructure.*** DoD must jealousy protect its information sources, networks, and databases from attack, failure, and compromise. Three sections of this volume deal with the basic infrastructure of command, control, and communications (C^3) and its protection, including the Integrated Information Infrastructure, information operations and protection, and frequency spectrum allocation.

- The need to treat ***C^4ISR*** as a system. The United States must treat C^4ISR as a system and the elements as components of that system. This "systems of systems" approach to C^4ISR is imperative for integrating the many stovepiped systems in use today. Section IV of this report deals with C^4ISR as a system including an R&D acquisition strategy that will address a Joint Systems Engineering Organization (JSEO). Logistics is also addressed as one area that will benefit greatly from improvements in information superiority.

"HARD" PROBLEMS

The following topics capture the challenges imposed by asymmetric adversaries in their efforts to deter the effective use of superior military power by the United States and coalition forces. The tactics employed by these adversaries will include attempts to deny superior air power; deny regions of vital battlespace by employing SAMs; use various methods for cover, concealment, and deception to hide their critical assets; disrupt critical information systems through information operations; jam U.S. communications and navigation systems; and use commercially-based information systems to provide a local advantage. To meet these challenges the United States must be able to:

- Regain lost battlespace
- Find, target, and kill mobile/moving/fleeting targets
- Identify, assess, and destroy underground facilities
- Become capable of more effectively using and protecting the Global Positioning System (GPS)
- Develop the capability to more effectively utilize commercial information technologies

Lost Air Battlespace

Current U.S. strategy leans heavily on "air occupation" of adversary territory. This is driven in part by reluctance to place ground forces at risk and the need to provide early and continuous response. The proliferation of man portable air defense (MANPAD) systems has restricted lower altitude air operations. The lost battlespace will be potentially expanded to higher altitudes and ranges of 100 kilometers or more with the proliferation of moveable SA-10 SAMs. The immediate impacts have been reduced ability for visual targeting and laser designation in bad weather and increased reliance on GPS-guided weapons. The use of GPS weapons does not compensate for this lost airspace for movable or moving targets.

The United States must recapture this airspace by implementing a variety of innovations, all difficult. Protection against future MANPAD systems will be more difficult due to the introduction of imaging seekers (vs. hot spot seekers) and seekers in the 8-10 micron band in addition to current seekers in the 3-5 micron band. Imaging seekers are immune to flares and conventional laser blinking jammers. Wider use of "blinding" systems may be needed if this threat proliferates. Locating MANPAD systems is extremely difficult. Autonomous loitering weapons and networked distributed sensors will be needed. Near-zero flight time weapons and distributed smart land mines may also play in the ultimate solution set. Further, attacking SAMs will be essential.

The Suppression of Energy Air Defense (SEAD) problem is exacerbated by SAM-intelligent networking, emitter radiation control, active decoys, and mobility. Losing the extended airspace will largely giving up laser-targeted weapons as well as being precluded from visual identification prior to attack – a requirement of current political thinking. Mobile-target SEAD via GPS weapons will also be extremely difficult using current concepts. Harm attacks at longer range will be even more costly and less effective. Loitering killers like the Low-Cost Autonomous Attack System (LOCAAS), coupled with stand-in decoys like Miniature Air Launched Decoy (MALD) and new stand-in jammers, will be required. Unmmaned aerial vehicle (UAV) targeting systems like the Defense Advanced Research Projects Agency's (DARPA) AT3 (passive time difference of arrival multi-aircraft systems) will be essential. Advanced mobile SA-10s will also preclude Global Hawks and Predators from their planned battlespace, depriving forces of essential "close-in" tactical intelligence unless the United States reacts rapidly to this increase in threat.

Mobile/Moving Target Targeting

The first step in targeting is to find the target. A key need is to continue the development of U.S. surveillance assets in both quality and quantity and to enhance the ability for real-time exploitation of their data. Even when targets are found by surveillance and exploitation assets, the mobility of critical targets such as command posts, communications nodes, missile launchers, and SAMs has precluded U.S. forces from successful all-weather attack in SAM-protected environments. GPS weapons are currently not usable for such missions. Unmanned, loitering weapons like LOCAAS may be required if available and survivable. Terminal seekers on long-range autonomous weapons using synthetic aperture radar (SAR), laser radar (LADAR), or imaging infrared (IR) may be required. The cost of such seekers and the necessary (currently unproven) automatic target recognition (ATR) capability will deter such solutions. U.S. forces must get inside the OODA times of mobile targets to impact this problem.

The obvious solution is the use of mid-course updates to retarget GPS terminal coordinates as close to impact as possible. Given an extensive near-continuous tactical sensing capability of mobile targets, and the Integrated Information Infrastructure capability to update target data in real time, the final link of weapon re-target becomes the long pole in the tent. Certainly, pre-flight GPS weapon targeting must be replaced by in-flight re-targeting. From a survivability viewpoint, GPS weapons should be locked on to appropriate satellites prior to launch. It will even be feasible and advantageous to update GPS weapons in-flight to even further close the OODA loop shortfall. Such concepts not only allow for moveable target attack, but potentially moving target attack. The data links required are low data rate and could provide additional GPS enhanced anti-jamming capability in a jamming environment. These weapons with seekers or other sensors on board – such as LADAR – can provide real-time battle damage assessment (BDA) and tactical reconnaissance as well. All weather, affordable GPS attack weapons for mobile targets must also have additional anti-jamming capability to allow effective operation, as is the case for fixed target attack.

Deeply Buried Targets

A systems approach that combines near-continuous remote sensing, local networks of microsensors, and high-accuracy precision weapons must be developed to address this important problem. The characterization problem is the most difficult and will require a rich mixture of sensing modalities to assess activity, determine the functions, and identify the unique capabilities of an underground facility.

U.S. forces have clear air-to-air combat superiority and will not be challenged directly in air combat in the foreseeable future. DoD is developing long-range sensors and precision weapons to attack fixed air and ground targets and demonstrated that capability in Desert Storm and recently in Kosovo. The reaction to this effective capability has been the utilization of SAMs to deny airspace, CC&D to hide potential targets, and the utilization of underground facilities to hide critical capabilities for the production and deployment of weapons of mass destruction. Underground facilities have also been used to hide tactical military targets, but while those targets are hidden, they pose no threat to U.S. forces. On the other hand, chemical and biological production facilities, nuclear weapons facilities, and weapons staging areas are critical targets that must be located, characterized, and destroyed before they can effectively deliver weapons. The United States currently has some capability to locate potential underground facilities, very limited capability for identification of activities being conducted within a facility, and a limited ability to destroy or neutralize them.

NAVWAR

DoD systems have become more and more dependent on the utilization of the Global Positioning System for precision geolocation, navigation, and time. All future precision weapons will utilize GPS/Inertial Navigation Systems (INS), and GPS is critical to the formulation of the common operational picture needed for command and control decisions. In addition, difficult problems like the location and negation of moving targets and the characterization of concealed or deeply buried targets will require distributed sensors and weapons which must themselves be precisely geolocated and georeferenced as well as accurately time locked.

The GPS signal is very low power and easily denied by an adversary. Without anti-jam capability, a jammer of modest power can cause GPS track loss to a weapons system, platform, or sensor system at significant range, while a very low power jammer can deny GPS code receiver acquisition. Since GPS is globally available to any potential adversary, DoD must develop techniques to protect U.S. systems using GPS, as shown in Figure 3, and to deny GPS to adversaries. Specifically, DoD needs to achieve 20 to 30 dB more anti-jam capability in GPS systems beyond the current practice. This level of improved performance would bring required jammer levels to very high power, making them targets. Techniques include improved adaptive antenna arrays (nulling, space/time adaptive processing; polarization nullers), deep integration of GPS/INS microelectromechanical (MEMS) systems, low-cost precise time for acquisition synchronization, and integration of GPS and wireless communications systems to utilize communications processors for longer coherent integration of the GPS signal.

In addition to improving the level of anti-jam capability in current GPS systems, DoD must develop its own capability to deny the use of GPS to adversaries. This capability will require the development of precision (high directivity) jammers. Therefore, DoD will need to develop a class of anti-radiation missiles to kill the large GPS jammers that adversaries will need in order to disrupt U.S. systems with improved capabilities to receive GPS signals.

In the long term, the United States will modernize the NAVSTAR satellite constellation with the goal of providing 30 dB more signal power for military utilization. This will also require a new military waveform to ease acquisition of the GPS signal and deny that signal and the ability to interfere with the signal from any potential adversary. The DoD should also investigate passive geolocation techniques that utilize the proliferation of space-based assets and develop utilization techniques to allow for alternatives to GPS in U.S. military systems if GPS is denied by an adversary.

- ■ A long term technology strategy is needed to preserve GPS utility as the underpinning of Joint Vision 2010 and beyond
- ■ #1 Priority: user equipment anti-jam appliqués/systems
  - 30-60 db anti-jam. via diverse (robust) techniques
    - • Antenna arrays (nulling, pointing, space-time adaptive processing (STAP))
    - • Polarimeters (polarization nullers)
    - • Integrated GPS/INS (MEMs)
    - • Integrated GPS/Wireless communications -- Snap track
  - Lock-on before launch of GPS weapons (A/C infrastructure)
  - Low cost innovative GPS/anti-jam A/C installations
- ■ #2 Priority: modernize NAVSTAR constellations
  - 30 db goal for higher military signal power
  - Add civil signals to deter competing European Galileo system
  - Add new military waveform (Lm) to ease U.S. acquisition and adversary denial
  - Provide suitable civil frequencies for all navigation/landing (civil and military)
  - Alternative navigation signals (i.e. Geosats, Discover II, commercial)
  - Make GPS the national time standard
- ■ #3 Priority: a focused prevention/adversary denial program (precision jamming and jammer location/kill)

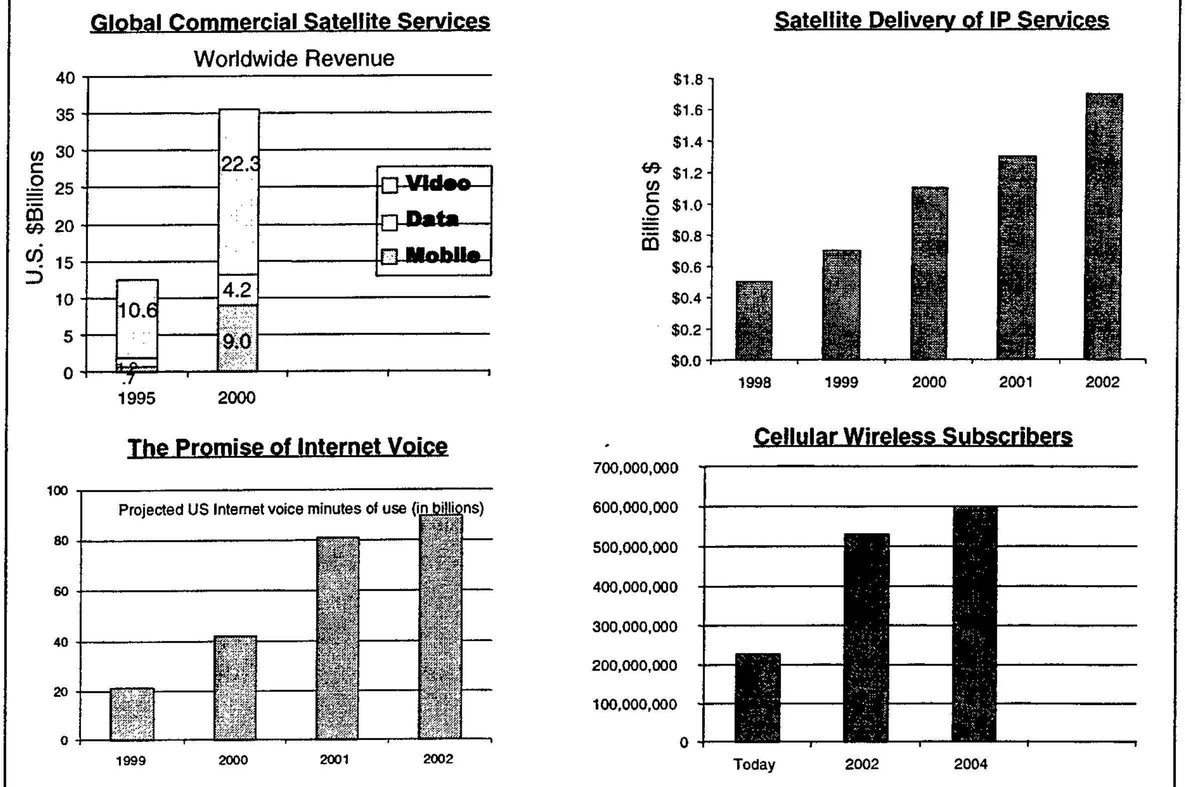
Figure 3. Priorities for Preserving GPS Utilities

COTS WAR

Emerging commercial information, communications, navigation, and imaging capabilities will allow potential adversaries to develop COTS-based military capabilities that could easily be more capable, timely, and dynamic than DoD C^4ISR systems, particularly when focused on the asymmetric approach to denying U.S. and coalition partners entry into localized hostilities. By continuing to take many years to field the latest commercial capabilities, DoD is giving potential adversaries, who can move much faster, a significant military advantage with technologies developed by the United States.

The proliferation of commercial technology worldwide, as illustrated in Figure 4, results in the availability of advanced communications, information system networks, and space-based surveillance and navigation capability to any potential adversary. The proliferation of commercial fiber provides worldwide access to wideband communications, and the development of commercial satellites with worldwide coverage (Spaceway, Globalstar, Teledesic) will allow access to global voice and data networks. The proliferation of the Internet and the expansion of wireless cellular systems will make robust, modern commercial communications and networking available globally. The proliferation of inexpensive GPS receivers allows anyone to geolocate and navigate with precision. The availability of commercial space-based imaging systems is also expanding. The new IKONOS satellite system can provide optical images to one meter resolution. Other commercial ventures (e.g., Space Imaging) propose to make one meter resolution and hyperspectral imaging available worldwide with very low latency.

DoD must recognize that the availability of COTS information systems is a major threat to U.S. information superiority. DoD must more effectively and rapidly use COTS information systems and develop the techniques and methodologies to deny their use to potential adversaries. This class of techniques falls under the heading of offensive information operations and must be aggressively addressed in close collaboration with attempts to make U.S. information systems more robust and less vulnerable to denial and deception by a potential adversary.



. . . Including among our adversaries

Figure 4. Growth in Commercial Information Technology

NO PLACE TO HIDE

CONTINUOUS, ON-DEMAND, SURVEILLANCE

One of the principal military lessons learned over the past decade is the importance of a robust, interoperable, C^4ISR system. From Desert Storm to Kosovo, operational commanders have highlighted the need for more continuous coverage of the battlespace in order to deny an adversary the ability to move and hide. In Desert Storm, the C^4ISR system was unable to provide timely synoptic coverage of the Iraqi theater of operations and could not support a lethal engagement of mobile ballistic missile launchers. In Kosovo, eight years later, the ability to provide synoptic coverage had improved, but the United States still did not have sufficient C^4ISR resources to maintain anything approaching continuous surveillance, and the system could not provide the capability to track and target time-critical, mobile targets. Most recently, the Commander, Allied Forces Southern Europe, in assessing the successes and shortcomings of the NATO mission in Kosovo, highlighted the need for "robust and sustained ISR...beginning long before [the conflict], and continuing throughout."

To address these needs, the Information Superiority task force foresees an increasing emphasis on continuous surveillance systems, with somewhat less weight on the periodic imagery reconnaissance now provided by national overhead and theater airborne systems. The debut of the Joint Surveillance and Target Attack Radar System (JSTARS) in Desert Storm and the use of video surveillance provided by the Predator UAV in Bosnia gave operational commanders some initial sense for the value of continuously tracking all movement within the battlespace.

During recent combat operations in Serbia and its Kosovo province, these capabilities were viewed as essential complements to the now routine signals intelligence surveillance provided by such platforms as the RC-135 Rivet Joint and the U-2, and continuous air surveillance provided by the E-3 Sentry AWACS. As a consequence, the task force believes overall airborne ISR posture needs strengthening and would be greatly enhanced by fielding additional airborne systems, both manned and unmanned. The operational use of technologies developed by the DARPA, under such programs as Moving Target Exploitation and Advanced Video Surveillance, would also enhance utility provided they can be successfully transitioned to ISR acquisition programs.

In moving toward a goal of continuous surveillance – offering an enemy "nowhere to run, no place to hide" – the task force believes UAVs offer great potential and their emerging capabilities must be more aggressively exploited. The Secretary of Defense has spoken out very clearly on this matter, stating in a July 1999 guidance memorandum to the Department that "the opportunity is here to develop, acquire, and integrate unmanned airborne reconnaissance vehicles into the force structure..."

Despite enjoying considerable success with reconnaissance drones during the Vietnam War, the military has, until recently, been slow to incorporate UAVs into the regular force structure. But because of recent UAV demonstrations – the Predator Advanced Concept Technology Demonstration (ACTD), and the Global Hawk ACTD flight test program – and the generally high marks accorded Predator and Hunter during operations in Serbia and Bosnia, the military leadership now views UAVs more positively.

A number of initiatives are underway at present which, if carried to fruition, will result in the ability of U.S. forces to field significant unmanned ISR capabilities within just a few years. These initiatives include a new tactical UAV (TUAV) replacement for the Army's Hunter, a vertical take-off and landing TUAV to replace Pioneer in the Navy and Marine Corps, and the joint Tactical Control System, which will facilitate cross-utilization of UAV sensor "take", and in some cases, flight/sensor control, between military Services. All are funded acquisition programs. Further, there are proposals to provide both Global Hawk and Predator with additional or improved sensors. The task force strongly supports these initiatives and urges that adequate funding be maintained for them as well as for building up a capable force of endurance UAVs – Global Hawks and Predators.

There remain two as yet unaddressed needs in the field of unmanned airborne reconnaissance and surveillance vehicles – one for a stealthy, high-altitude, long-range system, and the other for a low cost, high speed, under-the-clouds penetrator. The former would replace the DarkStar program that was cancelled early in 1999 because of concerns about its ultimate operational utility. Any decision on how to best meet these needs should be preceded by a thorough analysis that compares a proposed stealthy UAV against satellites and non-stealthy airborne reconnaissance systems.

The second of the two unaddressed UAV system types would be employed to obtain damage assessment imagery and pre-strike target intelligence under environmental and terrain conditions which limit or preclude employment of more conventional UAVs, satellite systems, and high-risk manned airborne reconnaissance assets. Candidate vehicles here include modified cruise missiles or aerial targets, the former Mid-Range UAV, a wholly new design, or the Bombardier CL-289, which the Germans and French used to good effect in Serbia. The task force believes the requirement for both system concepts merit careful assessment in the near term.

Approaches to addressing overall ISR requirements have not often led to optimum solutions because of the basic structure of funding within the National Foreign Intelligence Program (NFIP), the Joint Military Intelligence Program (JMIP), and the Tactical Intelligence and Related Activities (TIARA) Program. For example the combined global and focused theater coverage requirements for the Future Imagery Architecture (FIA) are not well suited for comprehensive collection from space for tactical support. There is not adequate funding for TPED, nor sufficient resources for high demand, low density, theater air assets (both manned and unmanned) that are traditionally funded within the JMIP and TIARA. In addition, independent ISR developments have not yet converged toward a sensor network that allows for the exchange of data between platforms. Such a network could eventually feed a distributed, heterogeneous, geo-spatially and temporally referenced database that preserves a complete record of collected and exploited data from all available sensor sources, along with the underlying pedigree of the information. As recently as the conflict in Kosovo, theater commanders were faced with over 30 different ISR systems that could only be integrated into a lose federation of collection capabilities.

Recommendations

The task force analyzed the continuing need for robust ISR in light of recent combat operational experience and concluded that three fundamental areas must be addressed in order to achieve a more continuous, on-demand, surveillance capability.

1. ***A coordinated sensor network architecture should be developed for sensor-to-sensor, and sensor-to-shooter, information exchange.***

The foundation of the continuous, on-demand, surveillance system should be an Internet-like connection between collection and exploitation systems that utilizes, and is compatible with, the Defense Science Board's proposed Integrated Information Infrastructure.[3] The Under Secretary of Defense for Acquisition & Technology USD(A&T), in coordination with the Assistant Secretary of Defense for Command, Control, Communications and Intelligence [ASD(C^3I)], should require that all future C^4ISR sensors and platforms be compatible with the Integrated Information Infrastructure, thus assuring interoperability and real time or near-real time dissemination of vital targeting information to shooters and their commanders. Research and development (R&D) efforts to develop the information management tools required to enable sensor-to-sensor and sensor-to-shooter data and information exchange should be pursued so that an initial capability can be realized by 2003. This initial capability should include connectivity between theater and tactical, manned and unmanned, moving target indication (MTI) radar sensors for shared track maintenance, and combined target quality tracking information. Of equal importance are the exploitation techniques necessary to extract information from the connected data sources. This is addressed later in the report.

2. ***New sensing modes should be developed, along with robust exploitation capabilities, to counter camouflage, concealment, and deception techniques.***

The capabilities of even unsophisticated adversaries to avoid U.S. collection systems require that new sensing techniques be developed. Because the utility of many of these techniques is not well understood, a broad R&D program across a wide range of applications should be pursued. Representative examples of such techniques are:

a) High range resolution (< 1m) moving target indication for target identification coupled with moving target imaging and cued stationary target imaging (relatively straightforward calculations show that these techniques will greatly reduce the overall requirements for broad area coverage SAR)

b) Advanced digital video techniques that embed targeting quality geo-coordinates directly in the video

c) Unwarned and unpredictable collection capabilities

d) Spectrally diverse and wavelength selective electro-optical sensors for detection and identification of targets practicing CC&D

[3] The Integrated Information Infrastructure is discussed in more detail later in this chapter and in Volume I of the Summer Study report.

e) VHF/UHF imaging and moving target tracking radars for identifying and tracking targets under foliage

The task force recommends that the Under Secretary of Defense for Aciquisition & Technology review the plans for developing these capabilities and ensure that available resources are adequate to undertake a broad R&D program in ISR sensor technologies.

3. *High demand, low density assets should be bought in greater quantities.*

The combatant Commanders-in-Chief have highlighted the need for more theater ISR systems – referred to as "high demand, low density" assets. These include a wide variety of highly capable manned platforms including (U-2, RC-135 Rivet Joint, E-8C Joint STARS, E-3 Sentry AWACS, EP-3E Aries II, P-3C Orion, E-2C Hawkeye, EA-6B Prowler, RC-7 Airborne Reconnaissance Low, and RC-12 Guard Rail). Eventually, the theater ISR asset pool will include a mix of various types of unmanned aerial vehicles including tactical UAVs, medium altitude Predator, and high altitude Global Hawk.

One approach to address the "high demand, low density" challenge is to transfer most requirements for broad area reconnaissance and surveillance to space assets. However, until new technologies to drastically reduce the cost of individual satellite systems are demonstrated – such as what could result from a successful Discoverer II program – the cost of fielding sufficient numbers of satellites to do this job will not be competitive with airborne collection. Unfortunately, as mentioned above, the current budget allocations between space and airborne systems are not balanced and do not reflect this cost-competitive reality.

The task force recommends that the Secretary of Defense relieve the intelligence community of the requirement to provide broad area, high revisit rate, imagery coverage in support of military operations until such time as new low-cost satellite technology programs, such as Discoverer II, are demonstrated to be successful. In the interim, the Deputy Secretary of Defense should ensure that sufficient resources are provided to procure additional "high demand, low density" ISR assets, including a robust production program for UAVs, especially Predator and Global Hawk.

Close-In, Covert, and Unmanned Collection

Adversary knowledge of U.S. remote-sensing capabilities combined with aggressive denial and deception and changing roles and missions has diminished the value of U.S. ISR systems. Today's ISR systems are cold war products designed to address a peer-level, superpower adversary in an era when peacetime activities (and anticipated wartime activities) were large in scale and difficult to conceal from sophisticated, powerful remote sensors. In sharp contrast, current and future adversaries are somewhat invulnerable to these systems for several reasons: proliferated knowledge of U.S. surveillance capabilities and weaknesses, construction of underground facilities for preparation and execution of actions hostile to U.S. interests, political and military strategies that can achieve goals while minimally exposing assets to U.S. ISR systems and weapons, and strategic weapons capable of threatening U.S. interests without warning from remote sensors.

Standoff ISR systems such as JSTARS, Rivet Joint, Guardrail, and overhead space assets are key elements of today's U.S. and coalition military capabilities against ground targets, and they consume a sizeable fraction of the overall defense budget. Military decision makers, recognizing the power of information and the pace of the information revolution, are planning for a future military even more strongly dependent on information than that enjoyed in Iraq, Bosnia, and Kosovo. Today decision makers are calling for more remote sensors to "close the gaps" and better remote sensors capable of functioning against moving and hidden targets. In addition, it is widely held that improved exploitation and wider, more timely dissemination of remote-sensed data will lead to "information dominance." While it might be argued that the vision of information dominance, as articulated in *Joint Vision 2010* and other forward-looking documents, can be achieved with more and better remote sensors, that alone is not enough.

Close-in sensing systems employed as a complement to traditional remote-sensing ISR assets will be necessary to extend ISR to the new approaches of potential adversaries. Close-in sensors, designed to operate at ranges on the order of one kilometer and less, can employ a wide variety of sensing modalities only available proximate to the source – chemical, biological, seismic, magnetic, and acoustic – in addition to active and passive imaging. Such systems can be remotely deployed, mobile, covert, and capable of high-bandwidth communications, all within a small package. As costs are reduced by new microsystems techniques, extreme proliferation becomes practical in the form of tens of thousands of remote sensors emplaced in bulk by air. New and emerging UAV systems might be employed to implant, monitor, and relay information from remote, close-in sensors. Perhaps most important, the ongoing revolution in micro technology promises to make such systems smaller, smarter, and more sensitive at lower cost – a trend continuing at least through the next two decades.[4] Close-in sensing systems could provide expanded capabilities that are robust to denial and deception due to unwarned sensing in multiple modes from multiple locations. Furthermore, such systems can be made affordably adaptable to a particular situation or to innovation among adversaries.

Analogous to the vision of Andy Grove (CEO of Intel) for the future of microprocessors, the task force envisions miniature, inexpensive sensors that are ubiquitous across a region of interest. Some of these sensors will seek out and tag targets, others will be scattered to monitor areas of interest hidden from the view of more traditional data collectors. A successful approach to close-in sensing requires investment in techniques for precision emplacement or location; covert attachment; low-power-low-probability-of-detection data exfiltration; exploitation and synergistic use with remote-sensor systems; and networking and exploitation integrated into real-time presentation. The technology of close-in sensing must be developed as a system, not as an assemblage of gadgets and trinkets that will never become an integral part of U.S. military strength. In addition DoD will need to accelerate its understanding and exploitation of new sensing modalities and non-traditional target emissions in order to maintain a lead in the ongoing sensor and anti-sensor arms race.

[4] Sensor systems the size of an aspirin tablet have been designed. The ultimate goal is one cubic millimeter sensor systems – so called "Smart Dust."

The cost to develop this 21st century sensing paradigm will not be inexpensive. The Task Force estimates a cost of approximately $100 –150 million per year for several years to coherently exploit a full range of new sensing modalities, develop the miniaturized sensing and communications, and explore emplacement schemes. This cost is inexpensive, however, compared to developing new traditional sensors that are becoming increasingly ineffective against adversaries with even a rudimentary knowledge of their capabilities.

The deployment of close-in sensors could be accomplished by airdrop, as in Vietnam, or by very small UAV platforms. The hand-emplaced devices can be seeded early by Special Forces or human intelligence resources in areas that have the potential to become problems. Peacekeepers and treaty monitors are ideal for planting leave-behind devices.

The simplest sensors would be seismic and acoustic devices that would be designed for minimum size and power drain, with a store and dump capacity when interrogated or flooded with radio-frequency (RF) radiation. Their function would be to count traffic (or identify traffic types) and alert other sensors to follow-up the activity.

The next stage would be a sensor that has the ability to "wake-up" when activity is detected. On-board processing of seismic and acoustic signatures would allow selection among items of interest that would be captured on a few digital video frames. The data would be transmitted on the next interrogation from the relay platform providing target identification, speed, and direction. Other on-board sensor elements would be awakened to watch for RF emissions that would trigger a counter to get the operating frequency and pass it on for automatic remote signals intelligence (SIGINT) collection.

Timeliness of reporting should be kept as a very high priority requirement since mobile traffic will be critical. Other on-board sensors could provide early warning of chemical or biological agents or increase in background radiation from passing nuclear weapons.

In the future, MEMS devices may allow access of close-in sensors that can force entry into denied areas of high interest such as communication centers and deep bunkers through air vents as "smart dust." These technologies should be strongly supported to develop an early capability in this critical area.

New techniques are required to provide precision location of sensors, particularly those dropped by air. One alternative could be achieved by translating the GPS RF spectrum to an offset frequency that would be collected and processed on a remote GPS receiver. The remote receiver would sort out the relative time difference of the relayed spectrum data. The processing center would automatically display active traffic and with time difference of arrival, provide an estimate of the source's location using both acoustic (affected by wind) and seismic transmission delays. Detection and precision location of firing weapons could be very helpful in heavy cover and urban areas.

A long chain of magnetic sensors dropped along power cable runs could help determine where power take-off occurs for underground facilities. The strength of the 50hz magnetic field is directly related to the level of current flowing in the lines. The magnetic field will drop as the end user tap is passed providing a technique for locating large underground facilities.

IMPROVED DYNAMIC INFORMATION EXPLOITATION

Dynamic information exploitation supports battlespace awareness, fire control systems and weapon seekers. This section describes a vision and goals for dynamic information exploitation, reviews the status of dynamic information exploitation technology, and presents findings and recommendations.

BATTLESPACE AWARENESS

Battlespace awareness is a high leverage area for the warfighter. A key element of providing battlespace awareness is high performance tasking, exploitation, and dissemination. However, the current tasking, processing, exploitation, and dissemination systems are inadequate for today's sensor data streams. This inadequacy has been demonstrated in multiple conflicts including, most recently, Kosovo. The existing TPED approach is essentially manual and for short dwell mobile targets the TPED system is totally inadequate. Enhanced threats and the forthcoming 100x increase in sensor data, while necessary to achieve understanding, will inundate the current system.

The goal of a dynamic information exploitation system is to develop and deliver the right information (not just data) at the right time to the right decision makers at all levels of command. To achieve this goal an effective system of sensors, databases, exploitation, and dissemination services must be developed. The continuous, on-demand, surveillance section described a vision including many networked sensor platforms all cooperating to keep ground threat targets continuously identified and in track. The long-term vision is a distributed dense set of networked, heterogeneous, collaborative sensor platforms (airborne, space-based, and land-based, including close in sensors) all supported by automated exploitation, fusion, and birth-to-death tracking of all targets and dissemination. The heterogeneous sensing and exploitation capability will thwart the threat's attempt to use CC&D to counter a single sensor. The sensing will be so dense that the threat will be almost continuously monitored and forced to stay in a deep hide state.

For continuous, on-demand, surveillance to provide battlespace awareness, significant automation improvements will be required in the ability to task collectors including self-cueing and cross-cueing of collection platforms (sensors and platform trajectories); to process sensor data; to exploit data in near real time including detecting, identifying, and tracking threats; and to disseminate extracted information quickly and in easily assimilated formats. Dynamic tasking, automatic exploitation, and tailored dissemination will no doubt be the critical issues in achieving the continuous, on-demand surveillance vision. Although all of these issues require development, exploitation and to a lesser extent tasking are those currently requiring the most effort.

A nearer-term goal should focus on the synergistic use of high range resolution MTI-based Moving Target Exploitation (MTE) and SAR-based Stationary Target Exploitation (STE). This advanced MTI radar would provide broad area coverage and tracking and classification of movers via its high range resolution mode and motion pattern analysis. The SAR would be cross-cued to provide classification of stopped targets. The system of sensors would operate in dynamic self- and cross-cueing modes. Thus, for example, if a threat moved in such a way as to be obscured for one sensor, then another sensor that had a suitable line-of-sight to the target would be immediately cross-cued. The synergistic MTE/STE system can be self-contained in one system such as case of Discoverer II, the RADAR Technology Improvement Program (RTIP), ASARS Improvement Program (AIP), and Global Hawk (assuming a high range resolution MTI is added to AIP and Global Hawk) or could be obtained by coordinating multiple systems. If pursued properly, the task force forecasts an era of synergistic MTE/STE that will revolutionize surveillance and reconnaissance and produce the sought-after dominant battlespace awareness.

The operational challenges for a dynamic information exploitation system are shown in Figure 5. The goal is to produce a condition of consistent and full-time battlespace awareness. The problem is not just understanding the enemy threat situation but includes awareness of friendly and neutral conditions. This level of battlespace awareness is required to make *Joint Vision 2010* a reality, particularly with respect to the *Joint Vision 2010* themes of dominant maneuver and precision engagement. Needed improvements to sensor systems include:

- Dynamic, continuous, responsive, and synchronized tasking and collection management linked to operations
- Mostly automated sensor exploitation
- Multi-sensor data correlation, fusion, and near-continuous tracking
- A distributed, dynamic database with intelligent information retrieval services
- Wide band dissemination including the last mile to the warfighter
- Visualization techniques to enhance speed and accuracy of warfighter information assimilation

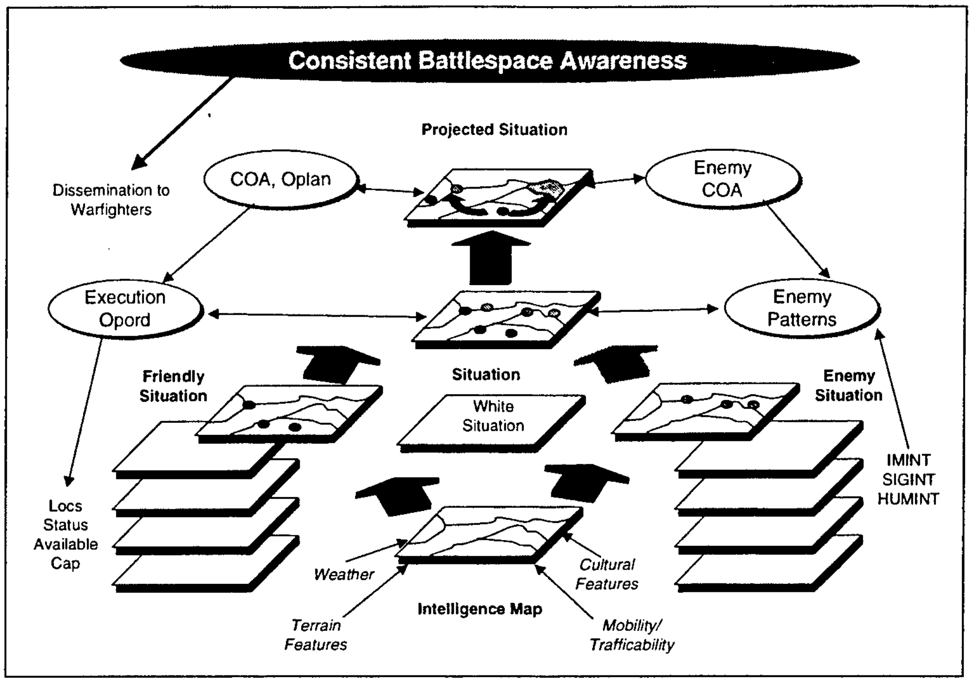
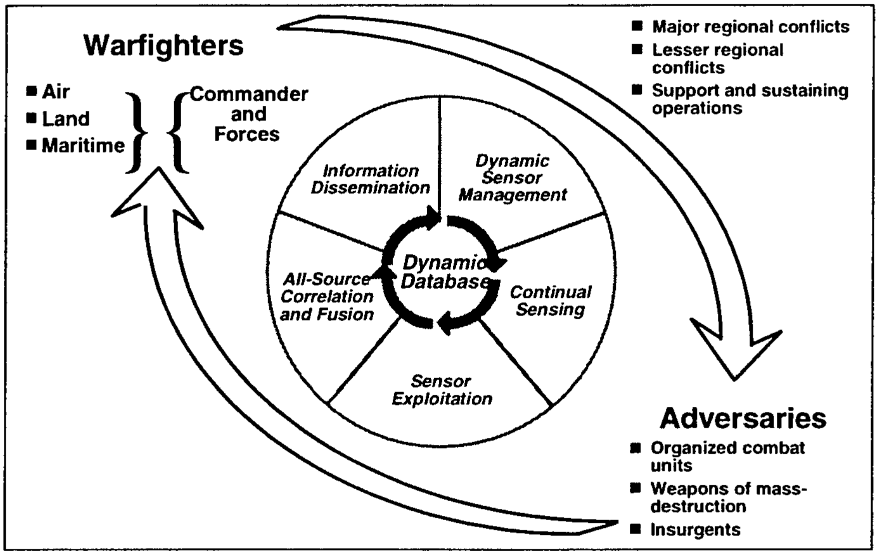


Figure 5. Battlespace Awareness

Figure 6 is a model that focuses on the key parts of the process.



Warfighters
■ Air
■ Land
■ Maritime
Commander and Forces
■ Major regional conflicts
■ Lesser regional conflicts
■ Support and sustaining operations
Information Dissemination
Dynamic Sensor Management
Dynamic Database
All-Source Correlation and Fusion
Continual Sensing
Sensor Exploitation
Adversaries
■ Organized combat units
■ Weapons of mass-destruction
■ Insurgents

Figure 6. Battlespace Awareness Challenges

The long-range technology challenges implied by this model are extensive and varied. The warfighter's needs drive strategies for tasking sensors to acquire the right information at the right time in synchronization with ongoing or anticipated operations. Sensors are needed which can observe the enemy while moving or stopped; in both day and night; in severe weather; under camouflage, concealment, and deception; and against complex backgrounds. The sensor platforms must support deep, near-continuous operation. Automated sensor exploitation technology is needed to convert sensor data from "signals" and "pixels" into relevant information (objects and activities) with a minimum of bad calls. Concurrently, the exploitation of the sensor data and its correlation and fusion must be managed and controlled to serve the warfighter. Correlation and fusion technology is needed to maintain a synoptic portrayal of the battlespace and to extract and track priority targets.

A common, geospatial-temporal referenced dynamic database must be maintained as the repository and process interface mechanism. Technology for maintaining dynamic geospatial-temporal databases is necessary to provide the glue for this system-of-systems. A visualization system must operate to support the warfighter's understanding of the battlespace situation. In the area of information dissemination, the ability to retrieve and distribute the right information to the right place at the right time, including getting the data over the "last mile" to the warfighter, is needed. It is important to understand the precise information needs of the warfighter, develop priorities corresponding to the overall national intent, and tailor the information to be provided to the supported missions and for the individual warfighter's assimilation capabilities as he "pulls" the information. Dissemination will require user interfaces that facilitate rapid and unambiguous understanding of the disseminated information. User interfaces will need to be tailored to mission objectives and perhaps even to individual users. It is anticipated that the development of appropriate user interface capability will become more like an Internet user today who creates a personal web page by searching out and pulling needed information.

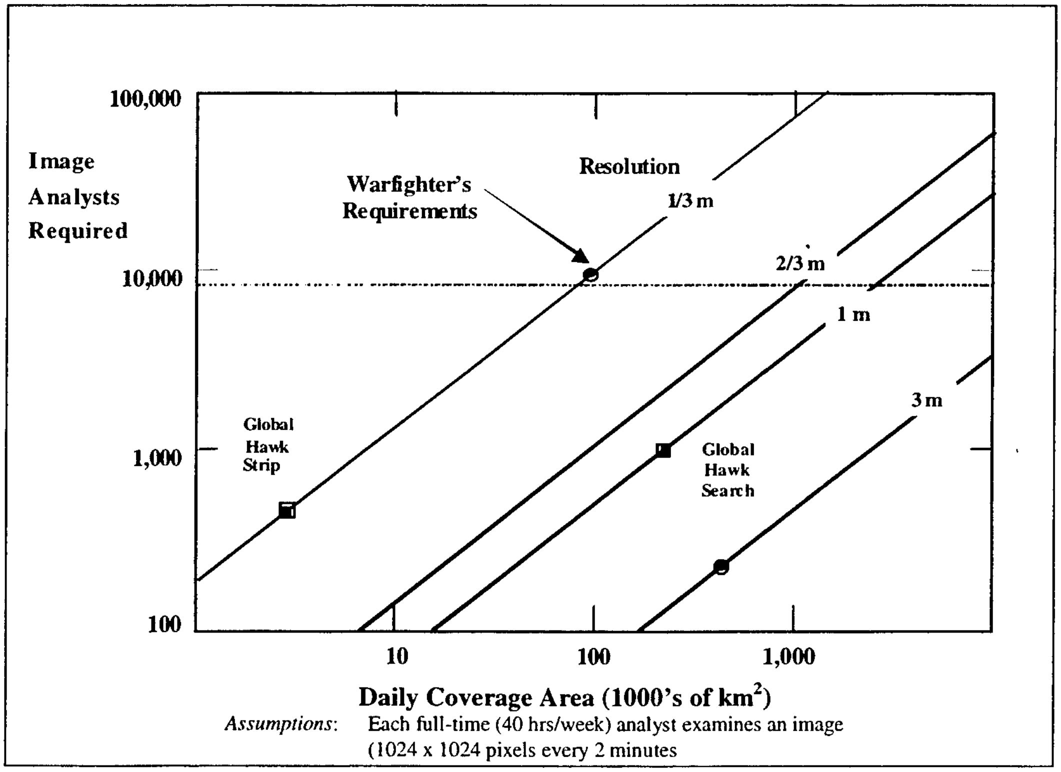
FIRE CONTROL SENSORS AND SEEKERS

In addition to capabilities needed to support surveillance and reconnaissance systems there are significant information exploitation requirements to support aircraft-based fire control sensors and seekers on weapons. For improved effectiveness and robustness and to avoid collateral damage, both fire control and seekers need high quality sensors and effective, highly dynamic exploitation services. Fire control sensors and associated exploitation processes need to be able to accept handoffs from surveillance and reconnaissance systems and to reacquire targets as necessary. When feasible, the fire control sensors can give independent evidence of the likelihood that the target is a threat. Also for a robust system it is desirable that the fire control sensor has some search capability in case surveillance and reconnaissance sensor handoffs are not available or are time late.

Weapons seekers need to have sufficient capability to accept a fire control handoff, acquire the target, and perform aim-point estimation and control. Desirable properties for seekers are to give independent evidence of the likelihood that the target is a threat and to support the navigation function presumably in conjunction with a GPS/INS. Another desirable property would be to have some search capability in case the fire control sensors cannot keep track of the mobile targets or communicate with the seeker after weapon launch.

SURVEILLANCE AND RECONNAISSANCE

To improve radar sensors for battlespace awareness, research and development in automating the image and MTI exploitation process is required. Figure 7 displays the number of image analysts required for a set of assumptions on image analyst processing time per mega-pixel image. In the future, when multiple U2 AIP, Global Hawk, FIA, and JSTARS platforms are simultaneously collecting data, the manual exploitation approach will require an unrealistically large number of image analysts. The software processing architecture and technology needs to support the image analyst by filtering out images with no information content and cueing the image analyst to regions of interest in imagery with threats. This is a critical issue that needs to be addressed by National Imagery and Mapping Agency (NIMA).



Assumptions: Each full-time (40 hrs/week) analyst examines an image (1024 x 1024 pixels every 2 minutes

Figure 7. Image Analyst Requirements

The tasking/collection management system is slow in obtaining a collection from a non-organic asset. National asset imagery collection systems are designed for a long-term, slowly changing allocation. This suffices for many of the intelligence community problems such as long-term monitoring of fixed targets. However, the system is too manual, and has too much latency to support many of the near real-time needs of the warfighter involved in a dynamic battle. The process for tasking theatre assets is similarly too bureaucratic and slow. Part of the problem exists within the military hierarchy, part in the national hierarchy, and part in the design of the sensor management systems.

NIMA's dissemination effort involving its data libraries is progressing well and the task force supports the continuing enhancements being made in this program. It would be preferable if MTI data and video were planned for an earlier insertion into the libraries. But the dissemination program fails to address the issue of the "last mile." The only plan for this need is to utilize existing tactical communications whose bandwidth is too low. The current dissemination system lacks bandwidth to echelons below the task force level. Although there is a high payoff for distributing imagery to tactical users it should be noted that these users are not well trained and they will need imagery analysis tools to aid their interpretation process.

Recently, NIMA has been conducting a TPED Analysis Program. Although the task force does not concur with some details of the models NIMA is using, it does concur with the conclusion that hiring more image analysts cannot solve the exploitation problem. Instead, a significant automation effort is needed. The forthcoming 100x increase in imagery will inundate current exploitation capabilities. NIMA's plans to initiate a much enhanced R&D activity in this area is encouraging; however, there is a long way to go.

The current TPED system is inadequate to support current and future warfighting needs. There is no evidence that the United States reconnaissance/surveillance/tasking, exploitation, and dissemination system and aircraft fire control sensor/exploitation systems have ever had much success against mobile targets other than in the simplest situations.

In the mid-1990's DARPA initiated a set of programs to develop information exploitation technologies to support battlespace awareness. A reference model for these programs is shown in Figure 8.

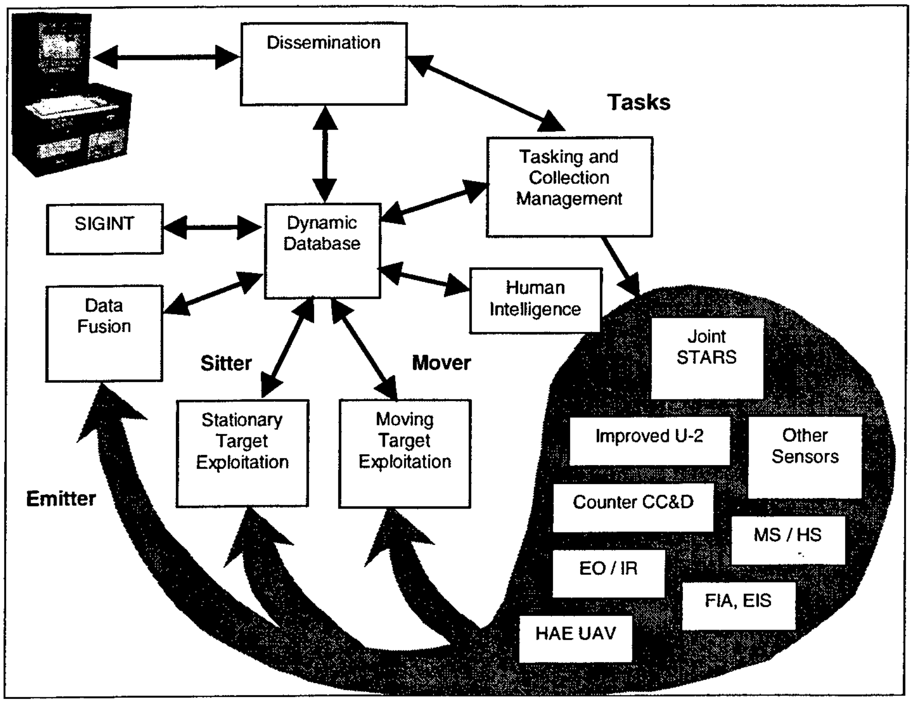


Figure 8. Reference Model for Information Exploitation

DARPA recognized that the forthcoming avalanche of sensor data would require major advances in exploitation technology. It also realized that the problem was difficult and would take a substantial period of sustained R&D funding to develop a significant capability. DARPA's program built upon prior activities conducted mostly by Service laboratories. The Services and the Defense Airborne Reconnaissance Office (DARO) supported DARPA's thrust, which included efforts involving base technology and infrastructure, applications, and system development. The system development efforts were primarily prototypes and occasionally ACTDs. Although considerable progress was made by DARPA, for the most part the technology still falls short of user requirements and necessary robustness. Relevant exploitation technology is not yet "on the shelf" except for targets in the open, in a standard situation.

Although some progress has been made in addressing targets in extended operating conditions such as articulated components, different configurations, and partial masking, significantly more work is required. In the tasking area some progress has been made in developing approaches for finding optimal collection platform trajectories and sensor schedules, given the prioritized tasking that has been assigned to a collection platform. However, progress is still lacking in appropriately connecting the warfighter's information needs to specific collector task assignments. Dynamic replanning technology is also lacking.

Recent key DARPA information exploitation and battlespace awareness application and system development programs include:

- Counter CC&D (CCC&D) to sense targets that are hiding in foliage or under camouflage and exploit the acquired data
- Moving target exploitation to track moving targets by MTI radar and recognize specific moving vehicles and formations
- Semi-Automated IMINT Processing (SAIP) ACTD to rapidly perform stationary target exploitation of imagery
- Moving and Stationary Target Recognition (MSTAR) to develop a robust model-based approach to vehicle recognition. In addition to targets in the open, it focussed on targets involved in extended operating conditions (EOCs), which included articulation, manufacturing variations of the same type of vehicle, vehicles in different configuration (such as with hatches open or extra fuel stores), and partial obscuration
- Dynamic Multi-user Information Fusion (DMIF) to combine diverse observations into force elements and targets, and to maintain long-term track histories
- Dynamic Database (DDB) to store and maintain a consistent, up-to-date, common geospatial-temporal referenced description of the battlespace, including intermediate and some raw products
- Battlefield Awareness and Data Dissemination (BADD) ACTD to solicit the warfighter's needs, retrieve appropriate information, and disseminate it to the warfighter when and where needed
- Advanced Information Management (AIM) to integrate the information needs of the warfighters and to manage sensors, exploitation, and fusion systems to produce and store the necessary information

The SAIP stationary target is an example of the state-of-the-art exploitation program. A view of SAIP's software architecture is shown in Figure 9. The SAIP design uses automated and semi-automated tools to detect objects of interest and eliminate false alarms. Stationary target exploitation (performed by SAIP) supports wide-area search by locating specific vehicles in imagery as well as military formations. SAIP was designed for a Global Hawk sensor that would cross-cue from its one-meter strip to its one-third meter spot mode.

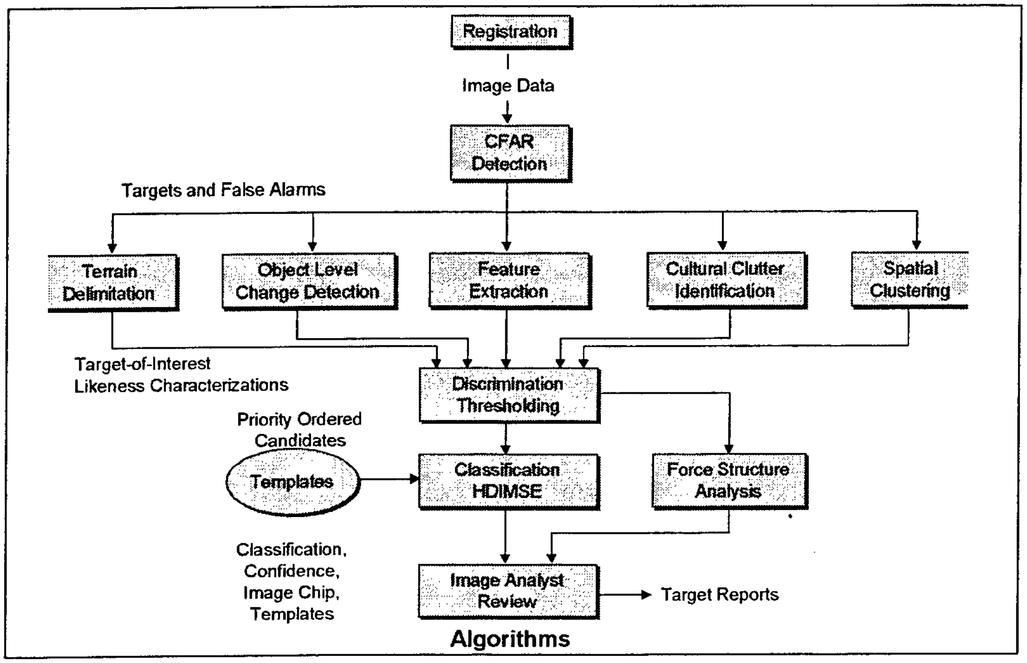


Figure 9. SAIP Software Architecture

SAIP's focus is on targets in the open. It currently uses a template-based ATR plus a set of false alarm mitigation techniques including terrain analysis and object level change detection. Template based ATRs are limited in their ability to address extended operation conditions. A parallel technology-based effort called MSTAR was initiated to develop a model-based ATR with the plan of subsequent insertion in place of the template-based ATR. Following the ATR stage is an interactive recognition stage in which the image analyst is cued to a region in the image to approve or disapprove the system's hypotheses. Fixed targets are monitored using a "site modeler" to determine changes between sequential observations, such as the presence of additional aircraft at an airfield or damage to a facility.

SAIP was demonstrated in Jan 1999 with a "sensor emulation platform" that emulated the Global Hawk sensor. Although SAIP fell short of promised performance, especially in the High Definition Imaging (HDI)/Mean Square Error (MSE) classifier area, the 18th Airborne Corp military intelligence user was quite pleased with the help it provided. The user is planning to obtain an enhanced version of SAIP in the future via a Joint Program Office that has been established.

A major contribution of the SAIP program was that it uncovered and helped quantify important synergies and interdependencies among disparate exploitation components – including terrain delimitation, change detection, and spatial clustering, for example – by emphasizing end-to-end system-level performance metrics. The SAIP architecture provides a validated framework for future exploitation systems and for the further development of exploitation technologies.

FIRE CONTROL SENSORS AND SEEKERS

FIRE CONTROL SENSORS

Modern SAM batteries, including shoulder fired SAMs with operational tactics that do not reveal their presence except right before launch, are quite stressful for airborne fire control platforms. Airborne fire control platforms are being forced to operate at higher altitudes and longer ranges than in the past to avoid these threats. This results in more requirements for sensors and dynamic information exploitation services.

Fire control platforms are typically cued to an area. For fixed or stopped targets only a limited search is required to acquire the target. In this case context plays a key role. If landmarks relative to the target location can be communicated to the pilot and navigator the search problem is greatly simplified. In the case of moving targets a larger search area must be covered. In some cases there is no cueing sensor available and the fire control platform must perform an unaided search for targets.

Because of platform size and the usual cued mode of operations, fire control sensors have lesser search capability than surveillance sensors. This simplification is more than compensated for by the demanding time lines, high functional performance requirements, and stressing environment of a high-performance aircraft. Given the many tasks of a pilot or navigator, who is acting as a fire control officer, a high degree of exploitation automation is essential. It is also important to provide context to orient the pilot or navigator.

Typical sensors employed include radar (SAR and MTI) and infrared such as Low Altitude Navigation and Targeting Infrared for Night (LANTIRN). Most existing sensors have serious resolution limitations. Rules of thumb for resolution are 30 pixels on target for detection and 300 pixels on target for recognition. These are not achieved for most current fire control sensor systems in typical scenarios. Exploitation on these platforms are a mixture of manual exploitation by the fire control officer plus automated cueing. Despite sensor limitations, the cueing systems attempt to cue the pilot or navigator to the target. The exploitation techniques mirror those used in surveillance.

For ground mobile targets the current operational fire control systems have not been successful due to a variety of potential problems, either individually or most likely in combination.

- The surveillance sensors do not collect at the location containing the mobile target or do not recognize the surveyed target
- Lack of timely hand-over to a fire control platform
- The fire control platform sensors do not collect at the location designated by the surveillance platform

- Inability of the fire control platform to recognize a target that it collects on

SEEKERS

Seekers typically support aim-point selection. In some cases they also support target recognition and navigation. Guided munitions have been used since Vietnam and range from artillery shells to long-range cruise missiles. The seekers include electro optical, imaging infrared, non-imaging infrared, wire guided, terrain contour matching (TERCOM), digital scene-matching area correlation (DSMAC), anti-radiation, and semi-active laser designators. They now often appear in combinations with a GPS/INS system. It is now widely accepted that guided munitions – such as weapons with a seeker and/or GPS/INS – are more cost effective than dumb bombs. Given concerns about GPS jamming more weapons are expected to incorporate seekers.

Some of the shortfalls in seekers are the lack of precision guidance in bad weather and smoke, length of the mission planning cycle, performance of the target recognition for mobile targets, and cost. The requirement for low cost suggests limiting the number of seeker types pursued so that DoD can achieve learning curve cost benefits. On the other hand, the desirability of matching the target type to the weapon, and robustness with respect to countermeasures afforded by a mix in seeker types, argues against too narrow a selection of seeker types. Thus a compromise is required. LADAR seekers are currently under development which can address several target sets including killing moving targets. Because of their high-resolution three-dimensional data, these seekers support accurate target recognition and aim-point selection.

Findings and Recommendations

IMAGERY AND MTI EXPLOITATION FOR BATTLESPACE AWARENESS

RESOURCES AND LEADERSHIP

The forthcoming streams of high-resolution data such as from the Global Hawk SAR (100 mega-pixels per minute for long periods of time) and MTI, Enhanced Imagery System (EIS) and FIA, will make the current approach of softcopy manual exploitation untenable. A major effort in dynamic information exploitation R&D is required not only to achieve the vision outlined but also to keep up with the currently planned data streams. Technology for rapidly screening imagery and cueing the image analyst to the small percentage of high information content images is imperative. There are opportunities to greatly increase system performance by developing and making effective use of all sensors and other data correlated and complementary to one another. In the radar domain alone, effective synergy of an advanced MTI with a high resolution moving target exploitation capability and SAR clearly will provide significant improvement. The exploitation community currently lacks an organization to lead this thrust to develop critical needed technology and systems. NIMA, with their current standards and architecture responsibilities, is a natural candidate to lead the exploitation community. However, the percentage of NIMA's resources invested in relevant R&D is grossly inadequate for an information systems organization. The percentage of their resources invested in R&D is only 3 percent of NIMA's total budget. Typical information system organizations invest 10 to 20 percent of their budget in R&D with 15 percent an average.

Recommendation: DoD should appoint a leader for the dynamic information exploitation community with responsibility for tasking, collection, extraction of information from previously collected data, exploitation, and the dissemination of results to users at all levels of command, for both the military and intelligence communities. NIMA should be given this responsibility. NIMA's a R&D budget should be increased to at least 15 percent of its total budget. Most (at least 90 percent) of the R&D spending should be outsourced and should not be earmarked for non-mainstream efforts. This budget should be fenced for R&D spending only. It should be understood that a sustained effort of a decade or more will be required.

NIMA should appoint an exploitation system architect at the deputy director level. NIMA should be given the authority, using mechanisms like the Intergovernmental Personnel Act (IPA), to hire new senior staff to help manage this R&D budget. The enhanced R&D group should be organized and empowered like a mini DARPA and report to the new deputy director. The organization and new talent should provide leadership and be an integral part of the information revolution in the military, with the goal of developing a new generation of advanced dynamic information exploitation systems.

SYSTEM ENGINEERING

The exploitation area lacks systems engineering. Solutions are often ad hoc. There is no evidence of systems-level or even exploitation processing software-level vision or corresponding architecture. There are no quality requirements analysis tools and as a consequence few quality requirements analyses are performed before exploitation systems are built. Dynamic battlefield and sensor simulations are typically not used to drive a model of the TPED process or to evaluate combinations of the collection, exploitation and strike systems in their ability to address the threat. Components of the exploitation system are not well understood nor are they usually subject to testing sufficient to characterize their performance in a variety of operating conditions. This component characterization is needed to support exploitation system modeling and requirements analysis.

Very few resources have been spent on developing a theory of exploitation or any of its components. Thus there is no theory to guide a system design process. Further the impact of alternate sensors on overall performance is not well understood.

Recommendation: A system architect for dynamic information exploitation should be designated and given the appropriate authority and responsibility over the community. Quality requirements analysis tools should be developed and utilized.

The system architect should develop a dynamic information exploitation vision and architecture and update it biannually. A set of performance analysis tools including simulation of a mobile threat with realistic terrain and motion models, collection platform and sensor models, exploitation models, and blue force models should be developed. This and complementary tools should be calibrated with information derived from training exercises, such as these conducted at the National Training Center. An on-going exploitation analysis process using this and complementary tools should be institutionalized.

Tools to allow tradeoffs between collection platforms, sensor characteristics, and exploitation methods should be developed. This should include the benefits of resolution, polarization, and multi-look by a single platform and multi-platforms. Tools to allow tradeoffs between collection, tasking, processing, exploitation, and dissemination investments should also be developed. The NIMA TPED analysis effort is a first step in the process but the scenario used in this analysis needs to be more dynamic.

RESEARCH AND DEVELOPMENT

Below some hig recommendations are given for high-level R&D thrusts. These specific programs are strawman suggestions for NIMA to consider. It is estimated that to execute these programs the NIMA R&D budget will need a $150-200 million plus up.

DYNAMIC INFORMATION EXPLOITATION

There are currently major shortfalls in most aspects of the dynamic information exploitation process. If the DoD does not act the exploitation capability gap will only get worse and the sought-for Dominant Battlespace Awareness will not be achieved.

Recommendation: A broad R&D program should be established that includes thrusts in developing operational prototypes (ACTD like efforts), applications (ATD like efforts), technology development, and the development of required supporting infrastructure. The operational prototypes should be built via a spiral development process and tested at military exercises.

Some of the exploitation programs that DARPA initiated should serve as a point of departure. As technology development efforts mature they should be migrated to applications and subsequently to operational environments. Technology efforts should migrate to applications. Applications should migrate to operational prototypes. Operational prototypes should migrate to operational systems. The focus of this thrust should be on the military problems of dynamic (i.e., real-time) tasking, exploitation, and information visualization.

A full-scale exploitation R&D program must include certain basic science components in addition to the development of software architectures and systems-level tests and demonstrations. For example, DoD does not yet understand how to determine the inherent information content of an image but such capability would enable more intelligent and efficient management of available exploitation resources. A broad-based R&D program should be structured such that it includes stable long-term funding for basic research and the development of new exploitation technology.

SENSOR EXPLOITATION

The sensor exploitation area is the one that is currently in greatest need of additional research and new technology development. As mentioned above one particularly promising area is the combination of Moving Target Exploitation (MTE - using high resolution MTI data) and Stationary Target Exploitation (STE - using SAR imagery). A concept of operation for the synergistic combination of MTE and STE is shown in Figure 10.

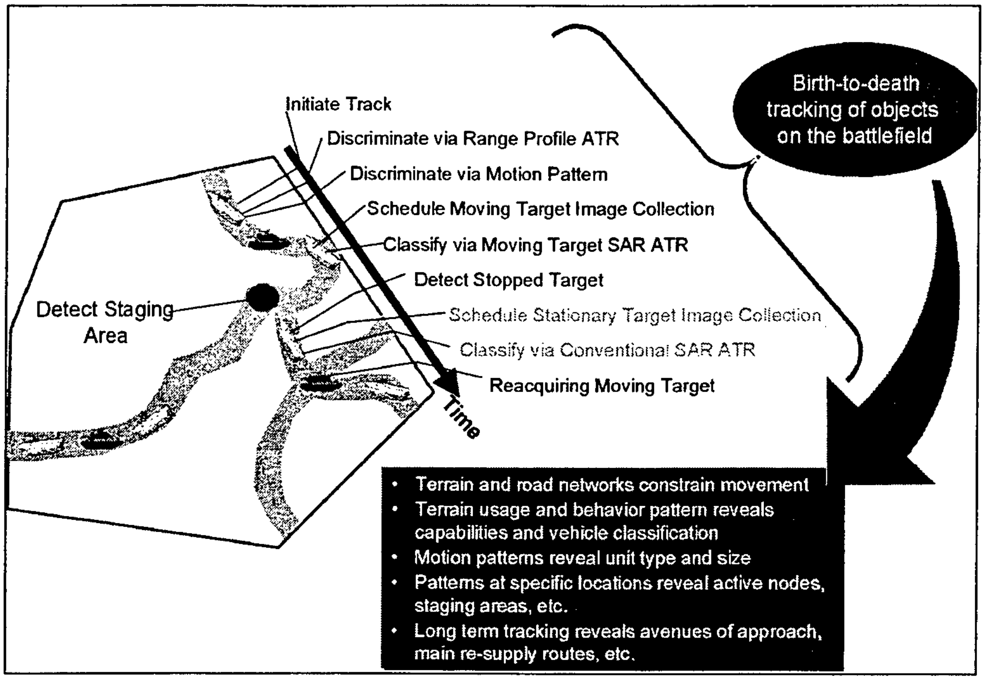

Birth-to-death tracking of objects on the battlefield
Initiate Track
Discriminate via Range Profile ATR
Discriminate via Motion Pattern
Schedule Moving Target Image Collection
Classify via Moving Target SAR ATR
Detect Stopped Target
Schedule Stationary Target Image Collection
Classify via Conventional SAR ATR
Reacquiring Moving Target
Time
Detect Staging Area
• Terrain and road networks constrain movement
• Terrain usage and behavior pattern reveals capabilities and vehicle classification
• Motion patterns reveal unit type and size
• Patterns at specific locations reveal active nodes, staging areas, etc.
• Long term tracking reveals avenues of approach, main re-supply routes, etc.

Figure 10. Synergistic MTE & STE

Related area that deserves serious attention is the use of MTI sensing for wide area search and/or indications and warning (I&W). A primary mechanism for I&W is the detection of change relative to previously observed norms. Area coverage, revisit rates, and processing requirements are considerably more favorable for MTI sensors than for SAR; however, MTI is not used for I&W, partly due to the lack of effective MTI-based change detection algorithms.

Among the limitations for SAIP is its focus on targets in the open, limited target set, and an under-performing template based ATR. The MSTAR ATR is quite promising and is a candidate to replace the SAIP template ATR. Among the limitations for MSTAR are its limited target set, use of instrumentation quality sensors, and its considerable computational requirements. Among the limitations for MTE is that it has not yet been demonstrated and tested in a military exercise. To accomplish this a demonstration van will have to be developed and a set of airborne collectors acquired or leased that have an appropriate wide band sensing and communication capability. The above limitations need to be overcome via a spiral development approach.

Recommendation: A series of research initiatives, application programs, and ACTD-like activities including the development of operational prototypes, experiments, and exercises in the exploitation area should be initiated. Research emphasis should be on uncovering and understanding the fundamental physical and phenomenological principles that govern the exploitation potential of the imagery and MTI produced by existing and planned collection systems, and on the development of new exploitation techniques and algorithms. The leader of the information exploitation community (NIMA) should maintain an extensive database of ground-truthed sensor data to be used by exploitation researchers in academia, industry, and government. As algorithms are developed in the research efforts they should be incorporated into systems-level ACTD-like efforts with the objective of exercising and testing the new techniques under realistic field conditions and with operational military personnel. The exercises should include joint warfighter and exploitation experiments at places like the National Training Center and Fort Hood.

The exploitation champion should assess the individual processing functions in SAIP (e.g. terrain analysis, image-to-image registration, object level change detection, force structure analysis, ATR, IA visualization, aided report creation), MSTAR, and MTE to determined their level of maturity and required enhancements. An exploitation system should then be designed, developed, tested, and demonstrated based on this and related assessments.

The exploitation community needs to develop a taxonomy of exploitation tools. A plan should be created for the development and integration of these tools. As required the funding of the champion's tool development effort should be augmented. The champion should deliver a capability for integration in an operational prototype. It is suggested that a review group be assembled to review plan for developing exploitation technology and an exploitation system.

TASKING

Improvements are needed for tasking national and theatre assets. A system needs to be developed that allows a low echelon military person, who has a high priority information need consistent with the commanders policy, to generate an information need and a corresponding tasking request through his military hierarchy and through a collection management function, and to achieve a collection from a sensor with coverage in a manner of minutes and not days. Also a system needs to be established to provide commanders with a feeling of "virtual ownership" of a portion of non-organic collection assets without sub-optimizing and having individual commanders only use assets they really own. Tools need to be developed to provide dynamic real time planning and replanning of all available collection assets including the cross cueing of MTI and imagery sensors.

Recommendation: A team led by DIA with members including NIMA, National Reconnaissance Office (NRO), National Security Agency (NSA), Central Intelligence Agency (CIA) and the military Services, should develop an execute a plan for a tasking/collection management system that supports the development of a warfighter's prioritized information need, responds rapidly to a warfighter's information request, and develops near optimal multi-platform trajectories and collection schedules for all available collectors. The system should include a rapid sensor cross cueing capability (especially MTI to SAR) to counter short dwell high value targets. For example, if an MTI sensor loses track on a high priority target because that target moved behind an obscuring hill, another collector with a more favorable viewing geometry should be tasked. This capability should allow systems such as Discoverer II or Global Hawk to cross cue FIA if FIA is in a favorable position. Also, tools are needed to ensure that collection requests for tactical, theatre, and national assets are coordinated and not redundant. Users also need better visibility into the collection plan and the status of requested collection tasks. Finally, work should also be performed on a user interface that can be tailored to support information search, retrieval, and warfighter assimilation. It would be nice if this interface had a lot in common with the one used for tasking.

Again it is suggested that this effort should include an R&D activity to overcome current limitations and a demonstration and evaluation in the form of one or more ACTD-like activities but with spiral development added. The proposed Defense Intelligence Agency (DIA)/CIA Community Intelligence Collection Management Program (CICMP) may provide a good system into which to insert this technology into.

DISSEMINATION

The dissemination effort sponsored by NIMA is progressing well. The task force supports the continuing enhancements being made in the dissemination program. However it would be preferable if MTI data and video were planned for an earlier insertion into the libraries.

One exception to the above view of the dissemination program is the "last mile" issue. No detail plan was presented for getting the information to the user other than to utilize existing communications whose bandwidth is too low. Although there is a high payoff for distributing imagery to tactical users, it should be noted that these users are not well trained, and they will need tools to aid their interpretation process.

Recommendation: A plan should be developed and executed by the Office of the Secretary of Defense (OSD) and NIMA to solve the "last mile" issue. The dissemination system including the information libraries should be tested for "industrial strength" and not just functionality.

MAPPING, CHARTING AND GEODESY (MC&G)

There are opportunities to correct missing and erroneous MC&G terrain features and elevation information from tactical, theatre, national, and commercial sensors just prior to and during a conflict situation, and to provide this information for operations and as context for exploitation.

Recommendation: NIMA should explore commercial, NASA, and other military sources to help develop these terrain databases. A non-trusted co-producer approach should be explored wherein the source of the data certifies a certain accuracy to the data; and NIMA samples the data, verifies this accuracy, and makes it accessible to users with caveats on the quality.

COMMERCIAL IMAGERY

One method of supplementing military collectors is to use commercial systems. However, there is no adequate plan to exploit evolving commercial collection capabilities.

Recommendation: Negotiate preferred deals with the U.S. commercial imagery providers which include real time access to their data. This deal making should be done soon while it is still a buyers market. Tasking, access, exploitation, and dissemination of commercial imagery should be a part of future military exercises.

INFORMATION EXPLOITATION FOR FIRE CONTROL SENSORS

Fire control sensors are emphasizing increased resolution to support higher confidence exploitation. Also more off-board data such as target imagery and models of the surrounding area are being forwarded to the cockpit.

Sensors being pursued on the R&D front appear quite promising. These sensors include improved resolution and higher power aperture SAR, high resolution MTI, forward-looking infrared (FLIR), multi-spectral, electro-optic and LADAR. There are also multi-sensor approaches such as SAR/FLIR fusion. The exploitation efforts for SAR and high resolution MTI for ground targets continue to build on similar ones for surveillance sensors. Improved results have been especially noted in the use of high resolution MTI for target recognition and for tracking.

The LADAR effort known as the Demonstration of Advanced Solid State LADAR (DASSL) is also producing impressive results. The goal is to do target recognition at FLIR detection ranges. The three-dimensional data provided by the LADAR is most impressive and with the developing model-based ATR should provide highly accurate and robust target recognition.

Progress is also being made in providing information to the fire control officer from off-board sensors/exploiters. The Air Force and Navy have complimentary programs on this subject, which go by names such as real time information in the cockpit, rapid precision targeting system and funnel navigation. Related efforts include on-board mission management, real time on board route planning, and sensor management. Also progress is being made in closing the sensor-to-shooter loop. These programs seem worthwhile and on track.

Recommendation: Given the promise of the LADAR effort and the LADAR's ability to support other sensors in resolving targets using CC&D, the task force recommends accelerating both the development of the LADAR and the exploitation algorithms. Also a broader technology base is needed for LADAR exploitation technology, including industrial efforts on the LADAR ATR and the current Air Force in house effort.

The task force further recommends more emphasis on fire control platforms using high range resolution MTI for tracking and classifying moving targets to support killing targets on the move.

Lastly, the task force recommends that the integrated communication systems to support two way communications from the strike aircraft be re-examined. This link needs to support both information in and out of the cockpit. Satellite communications, including the use of commercial satellites, should be a major consideration to support deep strike. For example, the communication links should support a Global Hawk to exploitation station to strike aircraft communication path.

INFORMATION EXPLOITATION FOR SEEKERS

A 1994 OSD sponsored study on a Assessment of DoD-Wide Terminal Guidance R&D advocated the following seeker selection for each of the five target sets mentioned earlier in this report:

- Fixed time critical hard target: Radar (either SAR or millimeter wave (MMW)) plus GPS/INS
- Fixed hard target (e.g. a bridge pier): LADAR plus GPS/INS
- General fixed target: GPS/INS
- Armor: LADAR or Acoustic/IR/IIR/MMW plus GPS/INS

- Dispersed target with location uncertainty: LADAR or Acoustic/IR/IIR/MMW plus GPS/INS

The seeker community seems to have focussed on these seeker selections and progress has been made in all areas. Note, the LADAR recommended here is a mono-static LADAR and not a LASER designator.

One change has been the advent of the Air Force's small smart bomb. Although bombs have the advantage of being low cost their typical heavy weight and the limited maneuverability of the Joint Direct Attack Munition (JDAM) kit results in the need for long-range target acquisition. Radar was selected because of its ability to acquire targets while the seeker is still above the clouds. With the advent of the small smart bomb and an improved maneuver capability there should be sufficient maneuver and a responsive enough control system to acquire the targets below typical clouds and weather. This opens up the possibility of the LADAR seeker for the small smart bomb to attack both fixed and mobile targets. LADAR seeker cost estimates are in the $10 to $15 thousand range per seeker. By using the LADAR to address some fixed time critical target in addition to addressing the fixed non-time critical hard target, armor, and the dispersed target with location uncertainty we increase the production volume and should further decrease the cost.

The results from the LADAR seeker on both the LOCAAS and the DASSL program are impressive. The seeker is designed to obtain 100 micro-radian data. At a two-kilometer range this corresponds to about an eight-inch angular resolution. The range·resolution is a few inches. This three-dimensional high-resolution data will support good performance for a model-based ATR. A reflectance channel can provide additional information. A new thrust for simultaneous receive beams from a focal plane array will speed up the scan rate. Since the LADAR provides independent evidence relative to other typical surveillance sensors it should support a nil collateral damage goal. Given the number of (3-D) pixels on the target there is also some robustness against CC&D. Because the LADAR is range-gated it also has some performance through smoke and in light rain (15mm). Note the LADAR also supports simplified mission planning, enroute navigation, accurate aim point selection, and it provides some indication of bomb damage. The LADAR, together with the 20-minute (120km) powered LOCAAS being developed, should provide a significant search area for fleeting or hiding mobile targets. The unit production cost goal for and all-up LOCAAS weapon of $30 thousand for a production run of 10,000 weapons is attractive.

Recommendation: Given the promise of the LADAR seeker described above, the task force recommends accelerating both the development of the LADAR and the exploitation algorithms. Also a broader technology base is needed for LADAR exploitation technology, including industrial efforts on the LADAR ATR and the current Air Force in house effort. The synergy between the LADAR seeker program and the LADAR as a fire control sensor program should continue. In addition the LADAR should be considered as a supplementary sensor on low flying surveillance UAV's.

FLEXIBLE TARGETING

Flex targeting is a term that means the ability to attack a high priority target in minutes regardless of conditions such as the weather, terrain, adaptive enemy, security, or dissimilar coalition C^4ISR resources. **This flex targeting capability is not available to us today.**

DoD's future fighting ability must not be centered on a single air and space integrated Air Tasking Order that requires 24 hours to plan and execute. Effects-based targeting has to be the objective of the aerospace campaign planners, as opposed to campaign-by-target list management, which means that a list of approved targets is managed on a day-to-day basis. An example of "Effects-based targeting" taking down the electrical grid follow a sophisticated target analysis, to get the desired effects measured in hours, days, weeks, or months. It assumes knowledge of when and where to hit the critical nodes in this network. This approach also assumes you have the freedom to go after targets in a near-simultaneous way and the political sensitivities to appreciate the value of each node. Political consensus must be behind the effect rather than focused on the target.

In short, DoD does not have the means to deal with this problem in an efficient way. This is not to say we do not that the high priority of time critical target capability is not appreciated. There are reported "40 plus" initiatives run by different program offices, different Services, and agencies – with little interaction – trying to solve this problem. In EFX98 and JEFX99, the Air Force tried to demonstrate the capability to deal with emerging targets using a battle control center while continuing to meet CINC and Joint Task Force (JTF) objectives. Both experiments showed that there is much more to do in this area.

As the ability to include space (Theater Downlink, MTI, Hyperspectral, EO/IR, SAR, LADAR, SIGINT, etc.) and information operations into the planning and execution phase of aerospace campaigns is improved, it should be easier to move quickly to one air tasking order and to resolve the present constraints of flex targeting. Flex targeting represents the core of an imbalance-of-power strategy, which promotes American global military primacy by means of flexible response. To this end, the United States should improve its capabilities to employ precision weapons, stealth, continuous on-demand surveillance, close-in covert and unwarned collection, new targeting processes and procedures, and dynamic information exploitation.

JCS Publication 2-0 *Joint Doctrine for Intelligence Support to Operations*, AFJPAM 10-225 Targeting Publication, *The Joint Targeting Process and Procedures for Targeting Time-Critical Targets,* and Air Force Pamphlet 14-210 *USAF Intelligence Targeting Guide*, all provide an excellent overview of the targeting cycle. Targeting is the process of developing and selecting targets in response to the commander's guidance, objectives, commander's preparation of the battlespace and scenario, and matching the appropriate weapon system to the target by taking into account existing operational requirements and capabilities. The targeting cycle concludes with combat assessment, which determines the effectiveness of operations in meeting combat or battle objectives and is the start of the retasking cycle.

This cycle, as shown in Figure 11, is excellent for fixed targets but should be modified for flexible targeting as shown in Figure 12.

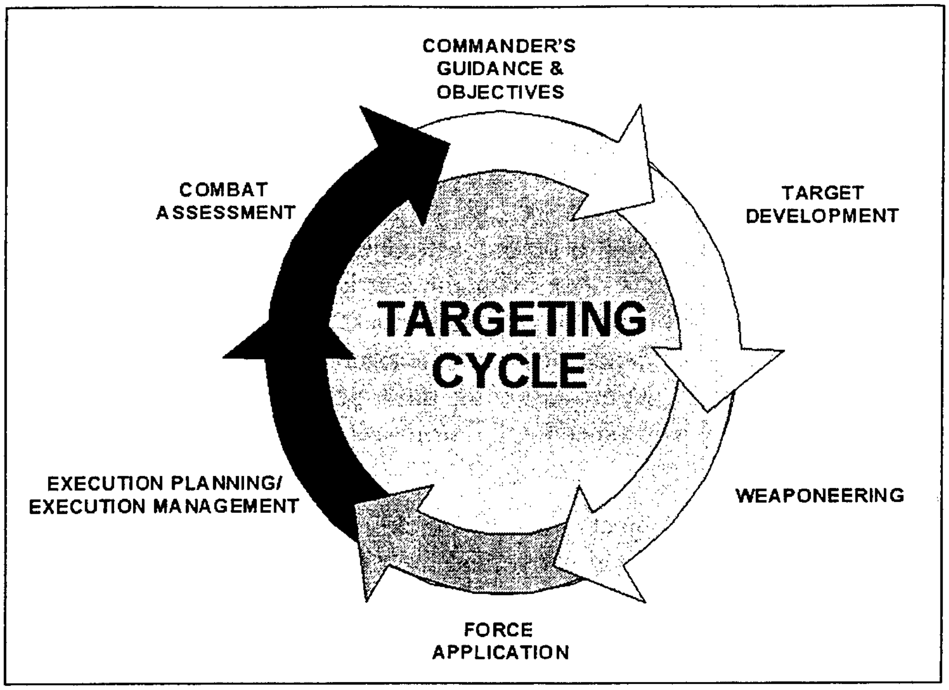


Figure 11. The Deliberate Planning Cycle

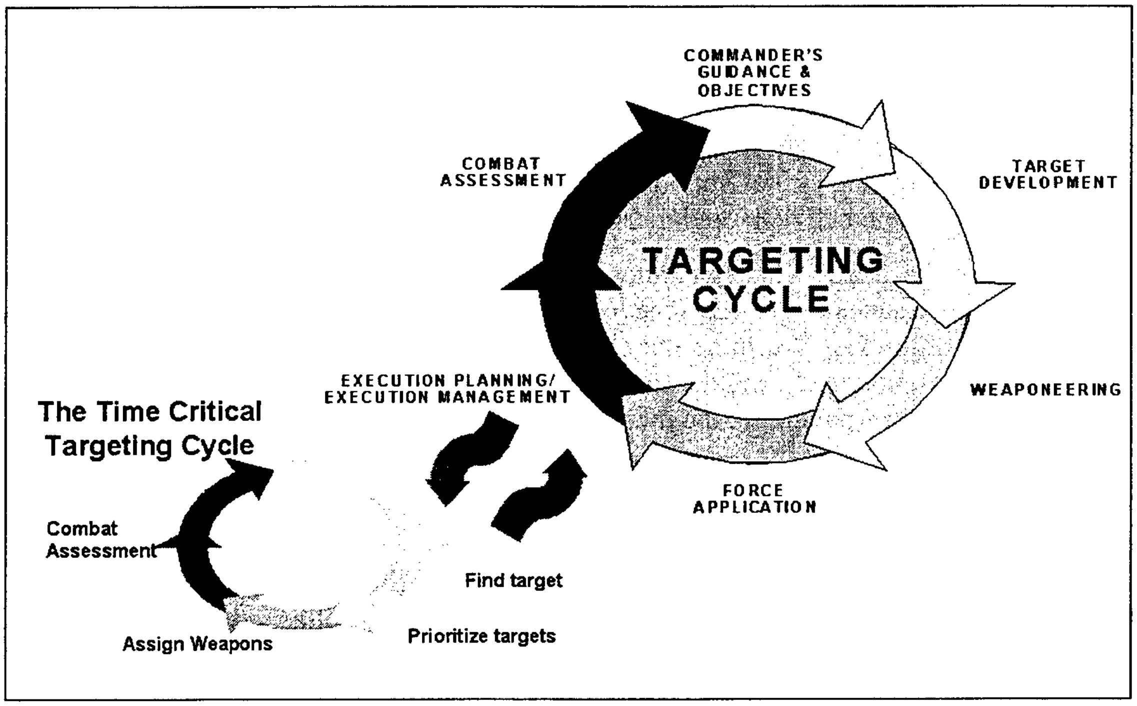


Figure 12. Deliberate Planning and Time Critical Targeting Cycles Where We Need to Be

For the United States to achieve responsive, effects-based operations the following steps should be taken:

- Build a continuously refreshing, staring, and dwelling capability with near-real-time and near-perfect picture of the surface battlespace (as we do for air combat today). We must orchestrate MTI, SAR, EO, IR, multi-spectral, etc., with Real time sensor scheduling and control needs to be orchestrated with MTI, SAR, EO, IR, or multi-spectral imaging to what is done with the Patriot, Aegis, or Joint STARS radars today. The current idea of collection management and intelligence collection as the targeting basis for surveillance and reconnaissance is not appropriate for the 21st century OODA loop. Dynamic targeting must be quickly adapted to a more time compressed process. The speed of information has to exceed the speed of engagement.
- All the relevant military objects must be quickly found and precisely identified from the operating picture described above and their four dimensional state vector (X,Y, Z, and time) qualities understood and tracked at high frame rates. (This is the world of ATR, noncooperative target recognition (NCTR) and the like, with much work remaining.)
- Next, using campaign plans associated with strategy-to-task effects based operations, along with the rules of engagement for any particular situation, the relevant military objects must be quickly and dynamically arranged into a prioritized and synchronized target queue.
- The target queue is then rapidly serviced with the weapons available by issuing a dynamic battle order (DBO). Weapons could range from input, output (IO) to many different precision strike options and could come from surface, air, and space manned or unmanned delivered means.
- As part of the DBO, which executes the weapon against the target, the surveillance and reconnaissance assets are scheduled and controlled to sense the employment of weapons to quickly determine the effects of the attack. The process is dynamically and quickly updated closing the loop (OODA driven). This is what we know as BDA today. Under this paradigm, the most important target is always on top of the queue.

The problem then becomes having a range of weapons available to service the queue. The air tasking order (ATO) becomes an “organize and dispatch” mechanism and not the targeting vehicle it is today. There is no such thing as a specific time critical target, since the most important target will always be on top of the queue and will be attacked with the best weapon available in the time frame needed to get the desired effects.

A common scenario required JSTARS to detect a moving target (current resolution required another sensor to confirm the target), cross-cue to a low flying Predator UAV with video, which in turn passed precise coordinates to a joint forces air component commander (JFACC), which finally alerted a precision-capable platform for the terminal engagement. In both Desert Storm and Operation Allied Force, the need for a responsive targeting, effects-based strategy/capability emerged as a critical operational challenge.

In both contingencies (Desert Storm and Operation Allied Force), the United States quickly moved from a strategic phase to an operational phase. Once in the operational phase the demonstrated ability to close between fielded target detection, identification, and classification to precision strike was inadequate. An adversary's field assets are the toughest to reduce because field assets tend to have reinforced armament and camouflage and move at frequent intervals. In Kosovo, U.S. forces did not have the necessary modes of sensors to verify what was and was not a legitimate target. However, even when legitimate targets were identified, U.S. forces could not engage those that moved inside their OODA loop.

There is a time value of war that permits adversaries more options. Neither national nor airborne sensors could provide responsive targeting information in sufficient time to permit negation of moveable targets. Simply said, adversaries are taking advantage of one of a key U.S vulnerability – a limited ability to engage and destroy moveable targets. The United States must minimize the effect of time working to an adversary's advantage.

This challenge requires advances in command and control, sensor webs, and engagement options that together extend flexibility and effectiveness well beyond what current and near-term systems can provide. The time scale between detection and munitions delivery must be decreased by an order-of-magnitude. A series of factors must be addressed in improving overall force effectiveness, such as capability, force implications, enabling technologies, and risk.

Command and Control Enhancement

Theater Battle Management Core System (TBMCS), with its initial operational deployment next year, is the future C^{4}ISR system for managing theater air in the joint or coalition environment. It leverages technology to implement synchronized joint air and space theater operations, which will provide for distributed collaborative air and space planning, execution, and assessment in support of integrated air, land, sea, and space operations. Using the Theater Air Planning Segment (TAP), TBMCS will perform theater level air battle planning and associate mission tasking with targets, thereby creating an air battle plan.

Now in its final development and testing stages before fielding, TBMCS will enable sensor-to-shooter operations. It has the ability to generate 1,500 plus missions within two to three hours. However, it must also be flexible enough to service any new target within minutes. To this end, TBMCS has incorporated a Time Critical Targeting (TCT) Cell that emphasizes intelligence and sensor capability to detect ground movers and kill them. This capability will be enhanced in future versions to include improved tools and additional capabilities including new capabilities to enhance timelines. What this means is that the near term TBMCS will actually have two targeting cycles, the "deliberate planning" cycle and the TCT cycle, as illustrated in Figure 12.

There is a renewed effort underway to develop operational concepts for the follow-on versions of TBMCS. A "way ahead" is currently being worked that will adhere to the operational and system level architectures that are being developed. These emphasize distributed operations and decision making. The operational concepts that describe the deliberate planning processes followed in an Air Operations Center's Combat Plans Division are well defined. Also, the emphasis since the Gulf War has been development of time critical targeting scenarios and concepts that are well defined for time critical targets (With a Missile Defense emphasis). On the other hand, operational concepts for combat operations are much less well defined and generally consist of a compilation of roles and responsibilities, not tasks with well defined nodes.

Combat operations remains a primarily face-to-face activity featuring phone calls and personal interactions. Combat operations tools in TBMCS play a prominent part in record keeping and alerts, but decisions to rerole and retask assets in the heat of battle are not made by tools, they are made through person-to-person interaction. The effect of collaboration tools on combat operations has shown promise, but its full effect on combat operations is a long way from being quantified.

The recent joint expeditionary force experiment (JEFX) featured a number of command and control initiatives, many of which enhance decision ability and reduce timelines. These prototype programs should be reviewed, evaluated, and if deemed effective, accelerated.

For example, one of these initiatives is the Attack Operations Decision Aid (AODA). AODA enables operators to monitor situational awareness and JFACC guidance, plan engagement options selecting from available assets, execute missions against TCTs, and assess the results. Its capabilities include rapid assessment of weapon capability and identification of the right asset to attack ground TCTs by highlighting the sorties that are in proper location, have the correct armament, and are not tasked to a higher priority target. It matches weapons and sorties to maximize effectiveness.

Another initiative is the introduction of collaborative tools. Two tools have been used, a commercial product known as "Info Workspace" and a government off-the-shelf (GOTS) application known as Collaborative Virtual Workspace. While the impressions from the use of these tools have been very positive, their effects on combat execution are still being evaluated.

Weapons Delivery Enhancement

One proposed solution provides for GPS ephemeris processing on the launch vehicle and near real-time broadcast of target location error updates to the weapon as late in the end game as practical. This approach will require a secure low bandwidth communications link between the delivery platform and the weapon, which allows the weapon to be retargeted in flight (vice just pre-flight) to neutralize moveable targets and also provides 20 db of anti-jam margin. This approach offers an affordable option to negate moveable targets and is more cost effective than expensive terminal seeker warheads using LADAR, radar or imaging IR sensors. Unattended ground sensors can also be used to fix targets in concealment or on the move.

In summary, many issues must be addressed to solve the flexible targeting problem. In addition, a lot of effort will be required to determine how to operate more effectively in coalitions. The task force has provided some near term recommendations to address part of the problem.

Counter-ISR and COTS War: The Adversaries' Use of Commercial-Off-The-Shelf Equipment and Systems

U.S. force planning and modernization, now taking place under *Joint Vision 2010*, relies heavily on achieving the objective of information superiority. Military force characteristics are being shaped based on the presumption of information superiority, and increasingly, are relying on that presumption as an integral part of U.S. force, doctrine and tactics. On future battlefields, it is likely that U.S. forces will require and use more information than will potential adversaries, and will be more dependent on that information in achieving military objectives.

Yet, as the world evolves toward a global community, U.S. potential adversaries are gaining much improved access to international, commercial developed information-related systems and disciplines, such as access to space, remote sensing, communications, navigation, and computing. Thus, achieving military dominance will require U.S. forces to fully exploit information technology and information operations to achieve the level of operational superiority envisioned by *Joint Vision 2010.* To do this, the United States must be aware of the potential for adversaries to access and use COTS systems, both to conduct their own operations and to disrupt U.S. operations. The United States must also be prepared to defeat adversary information-related operations and defend against their attempts to defeat U.S operations – these two areas defined as counter-ISR. The following paragraphs address each of these in turn.

Adversary Use of COTS to Conduct Operations

For quite a number of years, foreign military, terrorist, and drug groups have been using commercial communications, encryption, and SIGINT intercept gear to support their operations. These commercial products are highly competitive with U.S. military hardware across a broad spectrum from handheld radios and electrical power generators, to mobile satellite communications. With the use of these commercially available systems, the U.S. technical lead is being eroded.

COTS COMMUNICATIONS SYSTEMS

Some groups have taken advantage of very capable local and global communication network digital high frequency (HF) ham equipment to provide long-range packet communications. The very high frequency (VHF) and ultra high frequency (UHF) spectrums have also been used to direct combat units as well as for unattended mountain top relays. Problems of difficult mountain communication have been solved by using VHF and UHF ham repeaters, placing them and their storage batteries in automobile trunks, then driving them to mountain peaks, to allow communications in hard-to-reach regions of tactical interest. This equipment can be purchased to work outside the ham bands if it is not sold in the United States, but even the gear sold in the United States can be very quickly modified to provide different frequency capability.

There is a well-established pattern in the use of COTS communication gear. In air operations against Kosovo, U.S. flights were visually monitored from Italy, and this information passed to the Serbs by ham radio and cellular telephones. The KLA augmented communications with cellular phones and International Maritime Satellite (INMARSAT). The United States should expect to see this type of communication operation expanded in the future, with tactical use of terrestrial cellular phones and similar space-based systems providing a global capability through the use of low orbiting satellites. European cellular phones have very good encryption that further exacerbates the problem. This equipment is not designed according to military specifications, but its reliability, rugged construction, and extremely lightweight features make it very attractive. For added waterproofing, Ziplock plastic bags have been found to be quite acceptable.

COMPUTERS AND THE INTERNET

State-of-the-art desktop and laptop computers are now readily available to anyone, and the use of the Internet can bring any user global access. In addition to the Internet providing a ubiquitous communications medium it also provides access to a wealth of information that potential adversaries will undoubtedly find useful. In addition, adversaries may use this media to attack U.S. and allied networks and computer systems to deny service, disrupt communications, and provide disinformation.

GPS

Commercial GPS user equipment is readily available to adversaries for tactical use. The possibility also exists of using commercial GPS in the development of a cruise missile-like weapon or in many other weapon or platform applications.

SPACE AND AIRBORNE IMAGERY

Space-based photography suitable for surveillance purposes is available internationally from any of several foreign imaging satellite systems, such as SPOT, with additional commercial systems – including several U.S. space systems, such as Space Imaging – coming online in the near future. In addition, increasing amounts of imagery collected by space, airborne, and ground sensors are being placed on the Internet or in other public databases for public use.

LASER WEAPONS

Laser systems are being advertised in the commercial market for a variety of commercial applications. These systems can be adapted to serve on the battlefield to blind personnel and guide weapons among other things.

Use of COTS to Attack U.S. Operations

In today's world, the commercial market can provide to interested countries nearly anything they need to attack U.S. and other information systems. Modern commercial products can and do become part of the war chest of any user. Unfortunately, since adversaries are free to target whatever segments of the U.S. information infrastructure they choose, the United States must be prepared to defend against all attacks. Thus the economic exchange ratios often substantially favor the adversary. The following paragraphs address a few of the COTS-based options available to potential adversaries to counter U.S. operations.

JAMMING GPS

Although the U.S. has not yet experienced widespread use of GPS-jamming techniques in its military operations, U.S. weapons systems are becoming increasingly dependent on GPS-based navigation. Jamming the GPS signal could potentially defeat or render substantially less effective many U.S. weapons and support systems. Jamming the GPS signal over a relatively large tactical area – say, 100-200 kilometers radius – can be accomplished relatively easily with relatively low power (1-5 watts) jammers made from commonly available electronic parts. For example, a Russian company – Aviaconversia – offers for sale a portable, 4-watt GPS/Glonass jammer for less than $4,000. Others have demonstrated the ease of building effective GPS jammers by constructing jammers from commercially available ham radio parts. Deploying several of these cheap, easy-to-obtain jammers in a well-dispersed pattern could effectively deny U.S. forces use of the GPS signal in an area of operations. Such an approach would be difficult to defeat because of the jammers' dispersion and the relative ease with which the jammer pattern could be replicated. Many currently deployed U.S. forces do not have the means to quickly detect such measures. The implications of such jamming on U.S. weapons and tactics is discussed elsewhere in this report in substantial detail, along with several suggestions about how to mitigate this vulnerability.

COUNTERING U.S. ISR SYSTEMS

A recently published National Intelligence Estimate points out that all the U.S.-labeled rogue nations, as well as many other nations, now practice identifiable denial and deception techniques of one sort or another against U.S. ISR assets. For space systems, ephemeris data is routinely published on the Internet, even for classified systems. This information allows adversaries to simply schedule sensitive activities when U.S. satellites are not overhead. There are many simple CC&D techniques available that potential adversaries can often apply effectively to defeat the purpose of current U.S. ISR assets. The Serbs employed some of these tactics in Kosovo.

COUNTER GPS JAMMING

To counter the expected deployment of GPS jammers in the near term, DoD should be prepared to augment a theater with airborne and mountain top GPS RF sources. Five ground-based GPS devices (pseudolites) were installed in the Johnson Island Test Range to assure precision position information on certain missile tests.

Receiving antenna arrays with very deep pattern nulls on the horizon would be helpful if they were placed above surrounding scatterers. Higher satellite power and spot tracking beams are some of the GPS system modifications that need to be evaluated (and are being considered). The goal should be to raise the enemy required jammer power above 10 KW so that it becomes a “killable” target.

A SECURE INFORMATION INFRASTRUCTURE

THE INTEGRATED INFORMATION INFRASTRUCTURE

Decision superiority comes from the ability to leverage the quantity and type of information available about the battlespace and the forces within. Information is provided to the decision makers in a venue that enables them to make "good" decisions quicker than the enemy can do so. More timely and better-informed decisions will allow decision makers to operate "inside" the enemy's OODA Loop. This, in turn, will generate an operational tempo with which the enemy is unable to cope. This "information superiority" will lead to decision superiority, and ultimately, to execution superiority.

Information, information processing, and communication networks – collectively, a distributed information infrastructure – is thus at the core of virtually every aspect of military decision making and activities, as depicted in Figure 13. Improvements in the distributed information infrastructure enhance the conduct of these military activities and enable the overarching goal of early and continuous combat effectiveness facilitated through rapid, effective decision making. The task force, therefore, believes that establishing an Integrated Information Infrastructure is fundamental to realizing decision superiority.

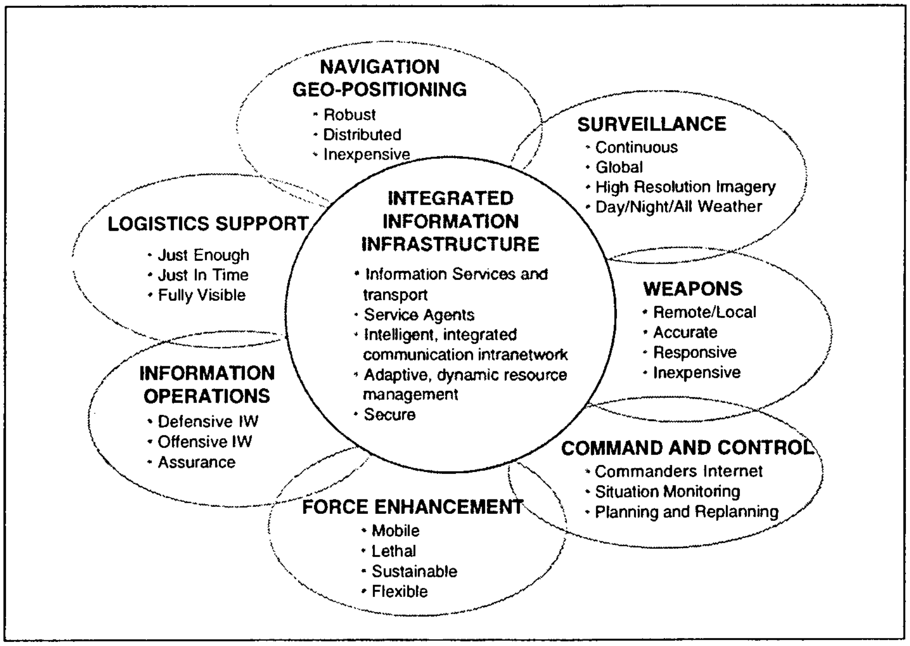


Figure 13. The Integrated Information Infrastructure - At the Core of All Warfighting Activities

To realize the benefits of the rapid-reaction operational concepts described in this report, the Integrated Information Infrastructure must be capable of reliable transmission, storage, retrieval, and management of large amounts of information. Today's C^4ISR systems are bound to specific communications systems/links, computers, and sensors that support specific functions, such as command and control, intelligence, logistics, and fire control. Importantly also, current systems are constrained by: (1) a lack of bandwidth necessary for high-resolution imagery transfer; (2) processor capacity needed for target recognition and interpretation; (3) memory sufficient to handle massive amounts of archival data; and (4) software to search the many data repositories quickly in order to provide commanders with tactical information in a timely manner. Such constraints are magnified by difficulties in operating a myriad of diverse legacy information systems in concert with newer service-unique and joint systems. These limitations can be overcome by integrating individual military C^4ISR systems into the interoperable Integrated Information Infrastructure.

A Conceptual View

The task force vision of the Integrated Information Infrastructure is that of a single infrastructure serving all users, and consisting of:

- A multi-tiered, multi-connected transport network
- A distributed computation environment
- Extensive use of software tools (browsers, search engines, and the like in the near term) and intelligent software agents (in the future) to help manage the infrastructure and the information residing therein

A conceptual view of the Integrated Information Infrastructure is provided in Figure 14.

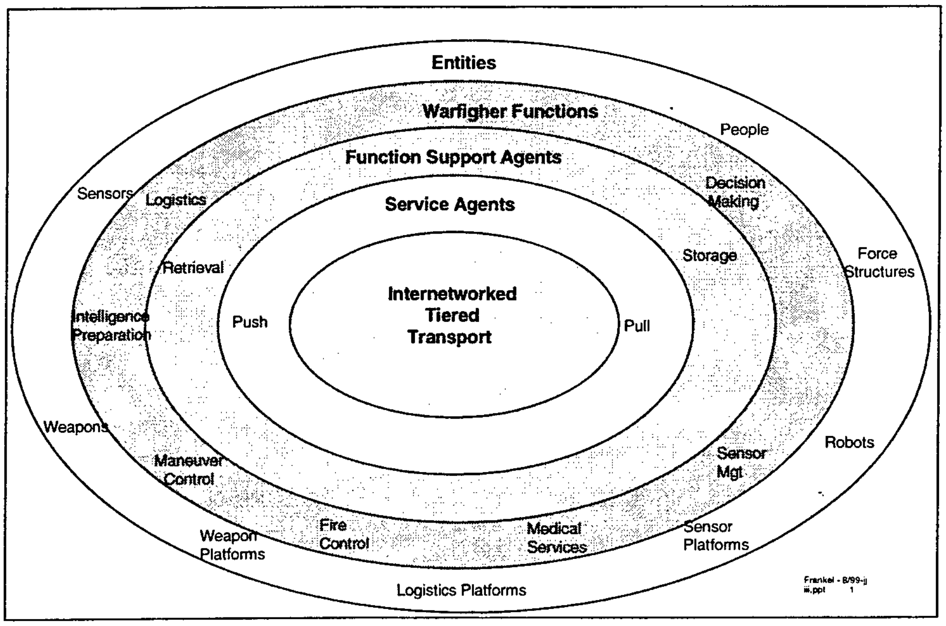


Figure 14. A Conceptual View

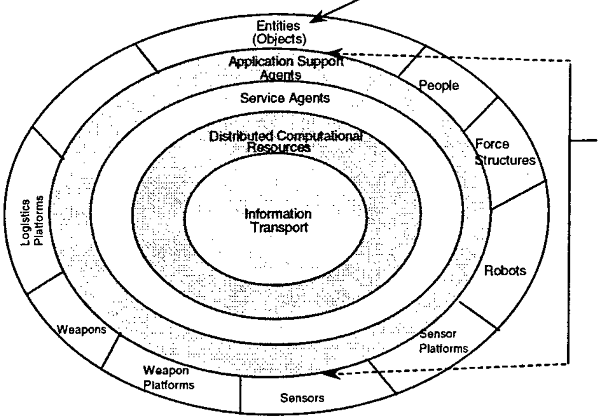
As stated earlier, and in *Joint Vision 2010*, a military force must be able to receive or transmit all of the information and command orders needed for successful and efficient prosecution of its mission, from any point on the globe, and in a system capable of rapidly adapting to changing operational and tactical environments. The Integrated Information Infrastructure must support these needs while allowing Joint Rapid Response Operations Forces (JROFs) and other forces of arbitrary composition to be rapidly formed and fielded. Further, the Integrated Information Infrastructure must adapt to unanticipated demands during crises and to stresses imposed by adversaries.

To support the warfighter's needs, the infrastructure needs to:

- Provide assured, robust command communications resources to all echelons
- Provide facilities to move information from any source to any destination
- Sources = sensors => eyes and ears of soldiers
- Information infrastructure = processors and communications => neural system
- Provide tailored information when and where required
- Automatic data storage, retrieval, and management
- Automatic data correlation and fusion
- Intelligent information dissemination
- Multimedia (images, video, text) information
- Facilitate force-structure tailoring
- Ensure the interoperability of all Service C^4ISR systems
- Close existing seams between military communication systems
- Close existing seams between C^4ISR systems within and between Services
- Provide robust, reliable information services
- Survivability through replication and self adaptation
- Quality of service to meet dynamic requirements
- Not place warfighters at risk of being detected and targeted

A System-of-Systems View

Figure 15 provides a system-of-systems view of the Integrated Information Infrastructure. At the center of the system is the transport layer that comprises land-line, wireless, and space-based elements. All these media are integrated into a ubiquitous, store-and-forward Internet work that dynamically routes information from source(s) to destination(s), transparent to the user. This data transport segment of the infrastructure is self-managing, adaptive to node or link failure, and provides services to its users based on quality-of-service requests. These services include bandwidths, latency, reliability, precedence, and distribution mechanisms (point-to-point, point-to-multipoint).



- Entities
  - Sources and users of information
  - Diversity of information needs
    - Type, quantity, timeliness
    - Change as a function of mission & situation
- Integrated Information infrastructure functional decomposition
  - Layered concept. Each layer:
    - Provides services to layer above
    - Receives services from layers below
    - Dynamically adapts to meet information needs of entities
    - Tightly coupled to each other to permit adaptation as an integrated system

- Agents = a software entity that is autonomous, is goal directed, is migratory, is able to create other entities and provides a service or function on behalf of its owner

Figure 15: A System of Systems View

The infrastructure will link the user to a distributed processing environment that includes many types of computers situated at locations appropriate with their needs for power, environment, and space. This distributed computing environment is integrated via the transport component of the infrastructure as shown later in Figure 17, thus enabling these processors to exchange data dynamically, share computation loads, and cooperatively process information on behalf of and transparent to the user.

The infrastructure integrates communication systems, computers, and information management resources into an intelligent system-of-systems. Layers of the Integrated Information Infrastructure exchange information with one another, thus enabling the entire system to adapt to user requirements and to stresses imposed on the network by an adversary. This adaptability also permits the infrastructure to change scale as necessary to support a revised force structure and to incorporate new processing, network, and communication technologies as they are developed. Hence, the Integrated Information Infrastructure is a scaleable computing environment.

The information infrastructure provides tailored information services to diverse users, ranging from a single person to a collection of people, sensors, and/or weapons. Here, intelligent software agent technology will play an increasingly essential role, functioning as agents under the general control of users. These agents will be goal-directed, migratory, and able to create other software entities, and provide services or functions on behalf of their parent users. They will proactively generate and disseminate appropriately packaged information. The agents will perform such functions as fusing and filtering information and delivering the right information to the right user at the right time.

Because computing resources are distributed throughout the infrastructure, the Integrated Information Infrastructure can readily adjust the amount of processing resources devoted to a single force entity. The entity's individual processor need only offer access to the infrastructure, provide an adequate interface to the user entity, and enable the acquisition and presentation of information to the user

To the maximum extent feasible, the Integrated Information Infrastructure's transport layer takes advantage of commercial technology and networks by utilizing open-systems standards and protocols that minimize the use of military Service or function-unique hardware and software. For applications where military-unique capabilities (such as anti-jam, low probability of intercept, or spread-spectrum waveforms) are required, military products will be developed or adapted to interface with the overall architecture.

The task force believes a foundation Integrated Information Infrastructure capability can be in place by 2005. This initial infrastructure would be comprised principally of DoD-developed legacy C^{4}ISR systems, augmented with commercial Web-based information management and dissemination technologies and with Internet-based telecommunication technologies. Over time, the Integrated Information Infrastructure would incorporate significantly more commercial technology, less military-developed systems, and technology derived from DoD-funded research and development that would focus on developing military-unique capabilities not available from the private sector.

As it evolves, the Integrated Information Infrastructure will enable these enhanced military capabilities:

- Geographic separation and functional integration of command, targeting, weapons delivery, and support functions
- Support for split-base operations, force projection, information reach back, combat, and force protection for large and small units
- Common situational understanding, common operating picture, and informed and rapid decision making for joint forces
- Enhanced operational flexibility for commanders at all levels
- Reduced logistics footprint in immediate combat area
- Full exploitation of sensor, weapon, platform, and processing capabilities
- Real-time or near real-time responsiveness to commanders' requests for information, fire support, and urgent logistics support

Example of Entities Supported by the Integrated Information Infrastructure

In Figure 15 we note that at the periphery of the Integrated Information Infrastructure are a collection of entities that share this infrastructure. Some entities post information into the infrastructure, other entities make use of this information for purposes of making effective, sound decisions or for the conduct of numerous other military functions. These entities are many and diverse, ranging from sensors to weapons to people. In all cases, however, these entities make use of the common Integrated Information Infrastructure.

For example, when the JROF must deploy, the Joint Task Commander, who has an Area of Responsibility (AOR), needs synoptic surveillance coverage of his AOR, shown in Figure 16 as the "Level I Bubble." This coverage is provided by a suite of sensors, "Sensor Mix I" – a mixture of sensors and platforms, e.g., assets in space plus a combination of high-altitude UAVs and manned aircraft. This enables the Commander to see his AOR and understand what's going on in a fairly precise way. Supporting that synoptic coverage is a second set of medium-altitude "Level II/ Sensor Mix II" sensors that provides greater resolution and a different sensor mix that search to locate the enemy and determine where it is safe to insert forces and logistics. And, finally, the combat elements, have an organic sensor capability called Level III/ Sensor III," which includes such capabilities as unattended ground sensors (UGS) and UAV-based sensors.

This sensor family provides continuous comprehensive situational understanding for all echelons of the JROF. The sensor mix does, however, raise the need to dynamically task and to manage the sensors and manage the information they generate.

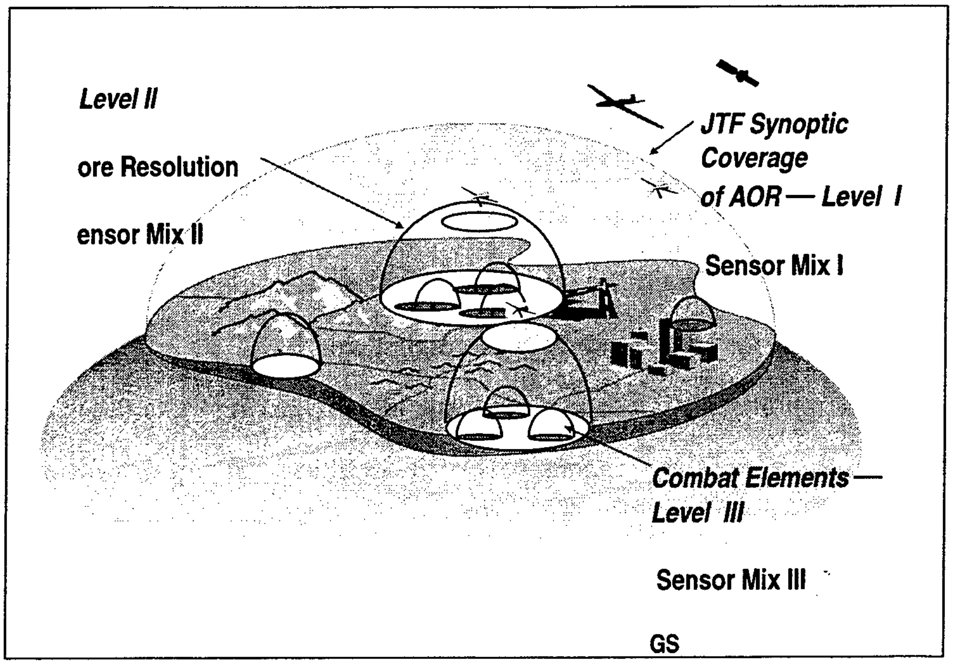

Level II
ore Resolution
ensor Mix II
JTF Synoptic Coverage of AOR — Level I
Sensor Mix I
Combat Elements — Level III
Sensor Mix III
GS

Figure 16: Decision Superiority: Creating Situational Understanding Capability

To meet this requirement, the task force proposes a "family" of sensors integrated into and managed through Integrated Information Infrastructure. A unique, stand-alone, sensor-specific communication system for these sensors should not be developed. Instead, the transport layer of the Integrated Information Infrastructure would be augmented, as necessary, to support these distributed sensors. By doing so, the information collected by these sensors would be immediately and automatically made available to other entities supported by the Integrated Information Infrastructure (people, weapons, ...). Similarly, dynamic sensor management and tasking commands would automatically be transported from the user to sensor-management software agents and then to the sensors themselves. This level of direct, fully integrated information transport, management, and distribution services do not exist today.

The Transport Layer

The transport layer of the Integrated Information Infrastructure is shown in more detail in Figure 17.

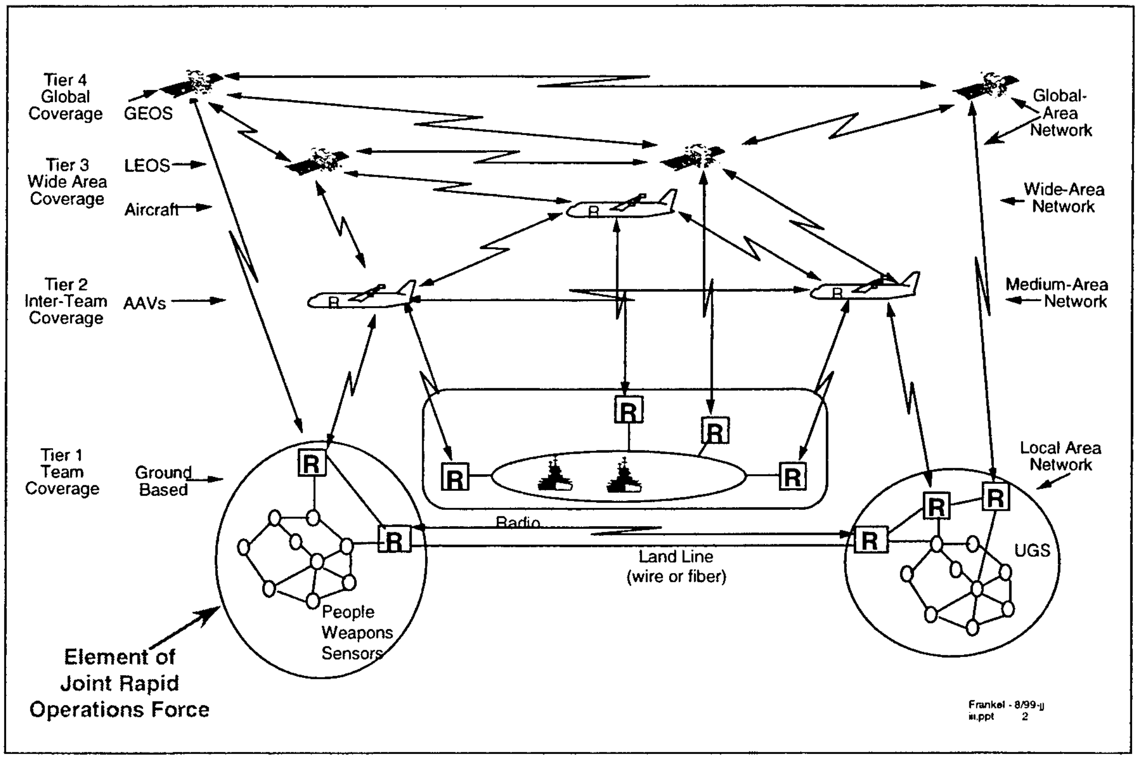


Figure 17. The Transport Layer of the Integrated Information Infrastructure

This multi-tiered, common user, quality-of-service-based layer of the Integrated Information Infrastructure must be provided sufficient bandwidth to permit information to be posted to the Integrated Information Infrastructure and any/all warfighters to compile their "information ensemble." The bandwidth and telecommunications services provided by the transport layer must be allocated dynamically and transparent to the user. Furthermore, all communication systems must be integrated, via commercial internet work protocols, into a network of networks.

The task force notes, however, that the bandwidth and telecommunications services needed to meet DoD requirements far exceed what it will be able to put in place if it follows its present communication acquisition strategy.[5] Unless greater use is made of a commercial-based systems, as the U.S. is doing in Bosnia and did in Kosovo, the military Services lack sufficient communication resources. In the Kosovo operation, the movement of data for targeting packages and video teleconferencing was supported through leased commercial communication systems. These commercial systems will only increase in number and capabilities in the future. For example, there is, in development today, several commercial satellite systems that will support bandwidth on demand and will employ active electronically-steered receive uplink and downlink antenna beams. Such systems include the geostationary-earth-orbit (GEO) ASTROLINK system, proposed by Lockheed-Martin, that will support about 7 Gbits/sec per satellite. This system will transport data at rates from 9600 bits/sec to 155 Mbit/sec. Teledesic is another example of a future wideband, low-earth-orbit (LEO) satellite system that will provide space-based services to users of the commercial Internet.

Given growing private sector investment in broadband, mobile telecommunication services via satellite, the question arises as to whether DoD should continue to buy DoD-unique satellite systems at substantial acquisition and ownership costs and for which ground receiver/transmitter terminals cost tens of thousands of dollars per unit. Or instead, should DoD leverage commercial space-based technology (lease or buy) which will deliver Mbit/sec to mobile users?

The trade space for providing an integrated transport layer for the Integrated Information Infrastructure is very complex. Many options exist for leveraging emerging commercial technologies and combining them with DoD-unique systems to provide robust, fully integrated, adaptive telecommunications transport services to the warfighter. A thorough, open, study of this trade space is essential in order to select the appropriate mix of technologies and systems for the DoD. However, it is clear today that the Department's present strategy of building DoD-unique communications systems/links to support specific military functions such as maneuver control, fire control, logistics, intelligence dissemination, and the like, creates intersystem and inter-Service seams that constrain joint interoperability and detract from the goal of decision superiority. It is also evident that the DoD-unique systems will not meet warfighter needs. The Integrated Information Infrastructure provides a vision for rectifying this situation.

To achieve decision superiority and the resulting military superiority, an Integrated Information Infrastructure is mandatory – it will be the foundation upon which distributed sensors, weapons, and people can be integrated into an effective and efficient warfighting system.

[5] See report from Defense Science Board task force on "Tactical Battlefield Communications" (to be released November 1999).

Implementation Recommendations

The task force strongly recommends that the Secretary of Defense direct development of the Integrated Information Infrastructure, with a target date for implementation in 2005. Implementation actions include:

A. Publication of a unified, joint technical vision for the Integrated Information Infrastructure

B Establishing a capstone requirement document for the Integrated Information Infrastructure

C. Establishing strategy, policy and plans for transition to the Integrated Information Infrastructure

D. Leveraging the explosive growth of commercial information technology

E. Maintaining targeted DoD science and technology investments to augment commmercial information technology as needed

F. Establishing a continuing program of experiments and simulations to evaluate and validate the Integrated Information Infrastructure, all under the aegis of U.S. Joint Forces Command

Further, the task force recommends the Secretary of Defense fix responsibility for Integrated Information Infrastructure development and *implementation as* follows:

G. Overall responsibility – Under Secretary of Defense for Acquisition and Technology [USD(A&T)] and Vice Chairman, Joint Chiefs of Staff (VCJCS), assisted by an Integrated Information Infrastructure Executive Office reporting to ASD(C3I)

H. Operational Architecture – VCJCS with Commander-in-Chief (CINC) and military Service participation

I. Technical Architecture – OSD(A&T), assisted by ASD(C^3I), military Services, and an information technology Advisory Board

J. System Architecture – ASD (C^3I) assisted by the Joint Staff and the military Services

Information Assurance

Protecting the Integrated Information Infrastructure is an imperative. Decision superiority will require defense in depth:

K. Improve DoD capability to characterize and respond to attacks on information systems

L. Seek legal authorities on response issues

M. Implement technical solution for identifying electronic point of origin of attacks

N. Develop special processes to address insider attacks

O. Establish response policy

P. Take immediate steps to dramatically improve DoD information warfare defense

Q. Policy to ensure access to all computers is by discretionary access control

R. Encrypt all unclassified traffic using strong commercial encryption such as triple DES

S. Develop an information operator in depth training program with certification

T. Embed a digital identification chip in every DoD computer

U. Ensure program to provide government-unique protection for critical systems

V. Make information operations readiness a CINC metric with periodic unannounced tests to assess compliance

The goal is to raise the bar to resist attacks. The technologies to accomplish this exist, but this needs to be implemented. The task force suggests a defense-in-depth approach to enable real-time detection of intrusions and anomalies, to protect the network, the data, and the system. Among the very critical areas of network protection to be addressed are network monitoring, actively countering outside attacks, protecting against malicious insiders (or errors), protecting information within the system with heavy use of encryption, and, overall, ensuring against denial-of-service and corruption of data.

DoD must be able to respond to attacks, recover from them, and reconstitute the networks, all of which opens up a wide range of policy and system challenges. The task force suggests that DoD define a minimum essential set of network systems that are absolutely needed, as was done in the nuclear era when the Minimum Essential Command and Control (MECCN) System was established. The task force recommends taking the same approach here.

The task force believes there are specific steps that DoD can take to improve its capability to characterize and respond to attacks on information systems. Legal problems have arisen with respect to response issues that need addressing. Technical solutions should be implemented for identifying electronic point of origin of an attack. DoD also needs to develop special processes to address insider attacks. A response policy must also be established.

There are some immediate steps that can be taken to dramatically improve the Department's information warfare defenses. For example, a policy should be put in place to ensure that DoD enforces discretionary access control to all DoD computers; DoD should embed a digital identification chip in every DoD computer; all computer traffic would carry the identification of the author. Also unclassified traffic should be encrypted using strong commercial encryption, such as triple DES to provide some protection to the formidable amount of information transported around networks as "unclassified."

The task force also believes that DoD should ensure that a robust encryption program continues for providing government-unique protection for critical network systems. There are government-unique steps that must be taken to protect critical and sensitive networks and data.

CINC-Space has been designated as the Information Warfare Defensive CINC. The task force proposes that the Air Force Information Warfare Defensive Capabilities, located in San Antonio, TX, be a backup site in case something were to happen to the CINC-Space site.

INFORMATION PROTECTION

Lessons Learned From Recent Operations

Recent operations point to a number of significant problems in DoD's ability to protect and defend information and systems. These problems stem from technical, procedural, and operational factors.

Despite the proliferation of secure telephones, monitoring efforts during both exercises and real-world situations indicate that personnel still do not make enough use of these instruments in their secure mode. The number of instruments does not seem to be a problem (at least among U.S. users); rather, it is the fact that many personnel still see secure communications as the exception rather than the rule, even in contingencies.

The proliferation of new methods of communicating has exacerbated the number of information sources available to adversaries. The increasing use of the Unclassified Internet Protocol Routing Network (NIPRNET)/Internet to conduct administrative business within DoD has spilled over into the operational realm. The benefits of e-mail – speed, delivery to a specific recipient, ability to communicate quickly with a wide array of people – have increasingly made it a means of operational communication. The same is true of other communications systems such as facsimile transmissions .and cellular telephones. Personnel often place convenience and timeliness over security in moving information; as a result, DoD is increasingly unable to control what information moves over what networks. All these systems are vulnerable to exploitation by relatively unsophisticated adversaries using relatively unsophisticated and easy to obtain equipment. The detail that can be can be obtained from unintentional sensitive information on these networks, and from aggregating even the unclassified information, pose a clear danger to U.S. operations.

The need for DoD to operate in a coalition environment further exacerbates information vulnerability. For example, DoD does not necessarily release compatible cryptographic systems to all coalition partners. As a result, there may be little use of secure communications between the United States and its coalition partners, and even less so among the coalition partners themselves. Thus, everything from mission planning to in-flight communications during air strikes may be conducted at the unclassified level. Second, the need to operate from overseas bases that DoD cannot fully secure makes U.S. information vulnerable to both technical and non-technical threats (e.g., close-in intercept of cellular communications, Human intelligence targeted against U.S. flight operations, etc). Third, the necessity to share a wide variety of sensitive data –

operational, targeting, intelligence – with foreign governments means that this information will be widely distributed within these governments. For example, the Air Tasking Order must be shared with recipients that may range from a nation's political leadership to its airspace control entities. In effect, DoD loses control of the information, to the point where U.S. decision makers may have no idea if, what, how, or to whom specific information has been released (or compromised).

Another emerging threat is the increasing use of computer networks to conduct offensive information operations. This threat can range from information attack to deception to psychological operations. At the outset of Operation ALLIED FORCE, for example, a variety of pro-Serb web pages appeared, some advocating attacks against U.S. and NATO servers. Other web sites were used to transmit Serb propaganda, including disinformation such as the purported loss of U.S. aircraft. At one point, pro-Serb web sites threatened B-52 aircrews and their families at Barksdale Air Force Base in Louisiana, to the point of listing the names of aircrews. Similarly, following the inadvertent U.S. bombing of the Chinese Embassy, DoD network protection organizations detected web-defacing activity emanating from China. In August 1999, similar use of computer networks occurred during tensions between China and Taiwan, with entities from both sides defacing web pages on their opponent's networks. In the future, as DoD faces increasingly sophisticated adversaries, such use of "cyberspace" for everything from denial of service attacks to corruption of databases to dissemination of propaganda will become the norm.

Some Recent Trends Impacting U.S. Information Warfare Capabilities

The United States has placed significant emphasis on information superiority as a force multiplier (in essence, the United States has "bet the farm" on using information operations to enable it to turn inside an adversary's decision cycle). At the same time, however, there are several trends that increase the technical and operational constraints placed on our ability to gain information superiority.

The requirement to operate within a coalition environment has a variety of attendant consequences that limit the ability to achieve information superiority. These include reduced interoperability among information systems (everything from radios to computer databases), the potential for compromise of information, the requirement to share data electronically with non-U.S. users and systems, and reliance on non-U.S. data and sensor inputs.

At the same time, the information infrastructure, which is essential to achieving information superiority, is increasingly vulnerable. More than 95 percent of military communications – computer traffic, facsimiles, wireless – travels via commercial networks, which are susceptible to a wide array of intentional disruptions. For example, a denial-of-service attack could affect not just unclassified systems, but secure systems as well if they use commercial communications networks. Additionally, almost none of the current DoD systems check the integrity of the data.

The United States has also reduced its tolerance for casualties, both among friendly forces and among an adversary's civilian population. This places increasing demands on intelligence to provide extremely precise information on enemy capabilities and force disposition. Potential adversaries recognize this and intentionally place civilian populations between U.S. forces and their intended targets, thus providing "moral hardening" of such targets.

Similarly, the development of increasingly accurate precision guided munitions demands an increasing level of precision in the targeting information collected and disseminated. In the Vietnam conflict, critical target nodes were identified in terms of target sub-sets (e.g., cracking towers at oil refineries, generator halls at power plants, etc). Today, precision-guided munitions require information with a much higher degree of resolution, accuracy, and fidelity in order to be effective. For example, it may be necessary to identify a particular room in a facility and then translate that location into mensurated coordinates to enable a strike by a GPS-aided munition with a small warhead.

The Cyber Situation Subset

DoD operates much of its information infrastructure on a network topology based on a local enclave, switching fabric and transport backbone. Enclaves typically contain multiple Local Area Networks (LANs) with computing resource components such as clients (users), servers, and local switching/routing, that transmit, process, and store information. The switching fabric contains components such as routers and switches which direct the flow of information through transport backbones. The transport backbones contain the transmission components (satellites, microwave, other RF spectrum, fiber, etc.), most of it commercially leased, to move information between the switching fabric. DoD employs the Internet and public switched telephone network backbone as well as the radio frequency spectrum for voice and data transmission.

Within DoD, data transmitted, processed, or stored in this networked environment is currently hierarchically "classified" as Top Secret/Sensitive Compartmented Information (SCI), Top Secret, Secret, Confidential, and Unclassified. In addition, information can be further tagged with a number of handling caveats. Also, DoD currently operates local networks at four hierarchical classification levels: Top Secret/SCI, Top Secret, Secret, and Unclassified. DoD supports these levels with three separated transport backbones: Joint Worldwide Intelligence Communications System (JWICS) for TS/SCI; the Secret Internet Protocol Routing Network (SIPRNET) for Secret, and the NIPRNET for Unclassified. The classified local networks are physically isolated from other local networks and information is encrypted/decrypted at the boundaries between the local systems and the transport backbones. Thus, information on local Secret networks is encrypted when transiting the SIRPNET backbone in one encryption net and information on Top Secret local networks is encrypted when transiting the JWICS backbone on another encryption net. The NIPRNET on the other hand is basically an open system.

In terms of network defense, DoD has focused initially on a perimeter defense approach, via intrusion detection, on the NIPRNET. Thus (at present), information defense translates – de facto – into computer network protection of only a limited portion of DoD's critical information services and systems. The service computer emergency response teams (CERTs) and the Joint Task Force for Computer Network Defense (JTF-CND), for example, have focused to date on detecting and resolving intrusions into DoD unclassified computer systems (i.e., those that use the NIPRNET/INTERNET) but not JWICS and SIPRNET. While the Services are addressing information protection through base network defense programs of their own, these efforts are not necessarily coordinated across the four Services. For example, the Air Force is implementing the Base Information Protection Program, the Information Protection Assessment and Assistance Program, the Operational Security Multidiscipline Vulnerability Assessment Program, and

Computer Security Engineering Assessments. The Army and the Navy have similar efforts underway, but none of the Service programs are compatible or interoperable.

Because these systems are unclassified, by definition, they do not carry information which, if compromised, would affect U.S. national security. In one sense, therefore, DoD is protecting its least critical networks. In reality, however, much of the information moved across these networks is sensitive, from both a privacy and a national security perspective. An example is the Global Transportation Network; another is information concerning the military blood supply. In addition, the aggregation of this unclassified data by a potential adversary can have a negative effect on national security if compromised. Therefore, the information needs some degree of encryption protection, ideally using devices approved by the National Institute of Standards. Until recently, however, there were a very limited number of these devices and the implementation was cost prohibitive.

It should be noted, however, that the bulk of the protection effort is devoted to defending the perimeter of the unclassified network as a whole, regardless of the sensitivity or criticality of the information on that network. The result is that non-critical information receives the same degree of defense at the perimeter as sensitive information, but there is insufficient "intranet"`protection taking place (e.g., there is no security within the local unclassified system). DoD computer defense organizations have no method of determining the criticality of networks under attack, except by contacting the user/owner of that network.

The fact that DoD's classified networks and their associated encryption backbones (JWICS and SIPRNET) are isolated from other networks has engendered a false sense of security. These local systems for the most part do not have intrusion detection capability or other "intra-net" protection, leaving them vulnerable to denial of service, viruses, or Trojan horses for example. At its most basic level, there are both technical and procedural factors that increase this vulnerability. These include the use of untrusted devices, unauthorized services, and poor security practices. Of equal concern is the insider threat. For example, on INTELINK any approved user has unrestricted access to an unlimited array of classified material.

Just as the classified systems are largely internally unprotected, the same is true of non-computer information systems. More emphasis is needed on ensuring that telephone switches, supervisory control and data acquisition (SCADA) systems, and wireless technologies are protected from intrusion, denial-of-service, or corruption. For example, base telephone switches are susceptible to a variety of threats such as war dialing, unauthorized probes into maintenance ports, and dial-up modem password cracking. Similar threats exist with regard to automated SCADA systems, which control power and water to DoD bases.

Protecting and defending the DoD information system requires the provision of a basic set of security services. These are: availability of the system (counter denial-of-service); integrity of information (counter malicious data manipulation); confidentiality of information (counter unauthorized disclosure); identification, authentication, and validation of parties in electronic transactions (counter spoofing and forgery); and non-repudiation (proof of participation in electronic transactions).

The fast paced evolution of information technology combined with the complex, widely internet-worked nature of the DoD information infrastructure dictates that no single solution can provide the security services defined above for the adequate protection and defense for all operational needs or for all environments. The majority of DoD information systems are interconnected such that a security risk to one entity is a risk shared by all those who are a part of the interconnected systems. Security is needed not only for intra-CINC, Service and Agency transactions, but also for transactions among the DoD components, and with other U.S. government departments, allies, coalition partners and commercial trading partners. Implementation of a defense-in-depth strategy (outlined below) – on a total enterprise basis – recognizes that, due to the highly interactive nature of the various systems and networks, any single system cannot be adequately protected and defended unless all interconnected systems are adequately protected and defended. Thus, a solution for any system must be considered within the context of the shared risk environment. This necessitates a comprehensive, common information assurance strategy be followed by all DoD components, who must cooperate in its development and implementation.

Recommendation One: Expand the Concept of Information Protection Defense

To adequately posture DoD against the growing threat to its information resources requires a broad, holistic strategy. This strategy includes the notion of "Protect" and "Defend." "Protect" includes those more passive activities associated with denying the adversary access to information and systems, and typically employs technologies and methods such as encryption, firewalls, and electronic. The notion of "Defend" encompasses passive and more active actions associated with an adversary attack, including attack warning, attack detection, and a variety of post attack responses. This latter area includes functions like adjusting/modifying protection measures, attacker diversion, attacker attribution, and electronic attack

The holistic defense-in-depth approach described above is built on three fundamental pillars: personnel, defensive operations, and technology. From a network perspective, the defense-in-depth strategy needs to mirror the DoD information infrastructure topology, providing layered protection and defense for the backbone and switching fabric, the perimeter boundaries between local enclaves and the backbone, and within the local enterprise environment. From a broader perspective, the defense-in-depth construct must consider all aspects of defensive counter-information (not just information assurance, but electronic protection, operations security, counter-PSYOPS, military deception, etc).

The first line of defense in this process is people. At the technical level, DoD needs to improve the recruitment, training, certification, and retention of personnel who use, operate, administer, and maintain information systems. In broader terms, DoD needs a more aggressive security awareness and training program for all its personnel. While personnel routinely receive foreign counter-intelligence briefings, there is no comparable process for ensuring they are aware of potential adversaries' abilities in terms of overhead reconnaissance, computer attack, signals intelligence, and related threats to information.

Defensive operations include defining and executing processes for creating situational awareness, conducting security assessments (e.g., red teams, multi-disciplinary vulnerability surveys, electronic systems security assessments, computer-to-computer monitoring), and incident analysis and response. As stated above, these defensive operations can be passive (e.g., shielding a particular operation from enemy observation through Operational Security (OPSEC)) or active (e.g., deception measures intended to mislead an enemy about an operation).

The third pillar is a sound technical framework. This translates to technical, performance, and best practice standards developed in conjunction with the information technology industry, which should be implemented employing a balanced application of government-developed and commercial security technology. This technical framework must weave through all DoD information warfare capabilities. Figure 18 summarizes the three defense in-depth pillars.

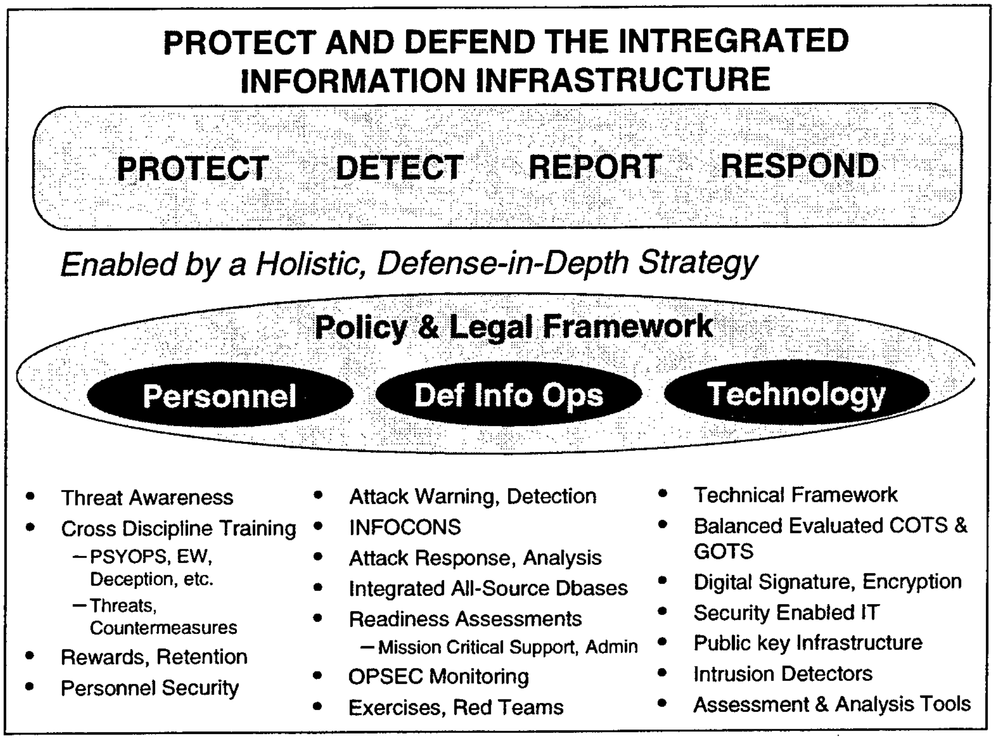

PROTECT AND DEFEND THE INTREGRATED INFORMATION INFRASTRUCTURE
PROTECT
DETECT
REPORT
RESPOND
Enabled by a Holistic, Defense-in-Depth Strategy
Policy & Legal Framework
Personnel
Def Info Ops
Technology
• Threat Awareness
• Cross Discipline Training
– PSYOPS, EW, Deception, etc.
– Threats, Countermeasures
• Rewards, Retention
• Personnel Security
• Attack Warning, Detection
• INFOCONS
• Attack Response, Analysis
• Integrated All-Source Dbases
• Readiness Assessments
– Mission Critical Support, Admin
• OPSEC Monitoring
• Exercises, Red Teams
• Technical Framework
• Balanced Evaluated COTS & GOTS
• Digital Signature, Encryption
• Security Enabled IT
• Public key Infrastructure
• Intrusion Detectors
• Assessment & Analysis Tools

Figure 18. Defense-In-Depth Pillars

To overcome the above vulnerabilities, DoD should do the following:

1. Direct the JTF-CND to begin developing a process and establishing requirements for tools to protect classified networks. For detection of intrusions, this effort should leverage the work already done in protecting unclassified networks and employ entities such as the National Security Agency and DARPA to develop solutions for addressing the unique needs associated with classified networks.

   a) An immediate step required is funding the hardware and manpower to install and monitor intrusion detection sensors at each of the trusted gateways connecting classified SIPRNET and NIPRNET networks together. This effort should leverage the current Secret and Below Interoperability initiative. This would provide information on attempts to gain access from the unclassified to the classified networks and allow monitoring of data passing from the classified to the unclassified networks (insider sending out information). Until automated data reduction tools can be developed, this may require additional manpower to monitor these devices.

b) Along with protecting these networks against intrusions, the JTF-CND must begin working immediately on tools and techniques and specify requirements to protect classified networks from insider activity. For example, automated systems must be developed that can detect and categorize anomalous activity by legitimate users on these networks. Establishing virtual private networks (VPNs) between all DoD components would ensure that all data traversing unsecured networks would be protected from outsider threat. It would also eliminate some of the hacker attacks seen today such as masquerading and some denial-of-service attacks. VPNs could also be used to form secure communities of interest reducing insider threats in both the unclassified and classified networks.

- As a part of its defense-in-depth strategy, DoD should ensure that its classified and unclassified network switching fabrics and transport backbones, including satellite technologies, the Internet Protocol (IP) routers, Asynchronous Transfer Mode (ATM) switching, and other emerging protocols, are adequately protected from denial-of-service attacks. Actions include: securing the satellite telemetry; tracking and control links; "hardening" switching fabrics by employing strong authentication on network management control commands to managed network elements (e.g. routers, switches) as well as on inter-element commands (e.g. router update table propagation). Achievement should leverage COTS security as much as practical, but also recognize that certain higher security needs will require government developed security. An example of this later case is the government developed Fastlane ATM encryptor which in subsequent releases will protect ATM cell routing information as well as mission data.

- Direct DoD agencies and the Services to work with the JTF-CND to identify the criticality of various networks – both classified and unclassified. While the long-standing hierarchical classification scheme is useful for identifying confidentiality needs, it is not useful in identifying needs for other Services, such as system availability, attack assessment, and data integrity.

a) This criticality categorization must include specifics about the information carried by the network, the applications on the network, users within that network, and the impact of a denial of service or corruption of data on the network. Such situational awareness (SA) of friendly networks ("blue SA") is necessary to allow the JTF to rapidly determine defensive priorities when it detects attacks against U.S. networks.

b) As part of this process, DoD elements must begin to identify the minimum essential network and information capability required to conduct operations. By doing this, the JTF-CND will be able to coordinate the reduction and elimination of non-essential services during an information attack and focus on preserving those capabilities critical to DoD operations. During recent operations, policies were established to "minimize" traffic on networks to "mission essential or mission critical." There were two problems with this situation: first, the policy was difficult to enforce and second, each individual organization determined what networks/systems were critical for its own uses (rather than determining which systems are critical to supporting a joint warfighting environment). To remedy this situation, DoD must develop a standard rule base to define the levels of criticality; one construct is to define systems as mission critical, mission support, or administrative.[6]

4. Develop "Wartime Reserve Modes" for information protection and defense. This would entail the creation of capabilities that are not used in peacetime (including exercises) and are therefore hidden from potential adversaries. Only at a certain declared Information Condition (INFOCON) would these capabilities be implemented. The intent is to confront an adversary with radically different operating parameters and systems so that his existing tools and techniques will be rendered ineffective, at least for a time.

5. Develop and enforce an overarching information protection and defense policy for all DoD – guidance, procedures, and funding security programs – to cover all information systems (networks, wireless systems, telephone systems, SCADA systems, etc). The on-going year 2000 remediation effort offers an opportunity to capture lessons learned about the vulnerability of DoD infrastructure to non-traditional aspects of information threats (for example, all U.S. bases are reviewing whether SCADA systems which support that installation are ready for the year 2000). The guidance promulgated by DoD must cover how these information systems are to be protected (such as level of encryption, firewalls and intrusion detection systems). For example, DoD should expand existing initiatives such as the electromagnetic security (EMSEC) program to address protection of wireless and cellular systems, as well as information assurance security programs to develop telecommunication infrastructure protection capabilities.

6. Direct that only evaluated and validated protection technologies and systems may be used by DoD entities. The proliferation of commercially available tools for network protection has resulted in a lack of coherence – and increased risk – in the information protection infrastructure. For example, the large amount of off-shore produced software has created concerns about embedded code that would allow back-door access or introduction of Trojan horses. In support of this activity, the National Security Agency (NSA) should expand its emerging commercial security product and system evaluation and validation process (in conjunction with its NIST National Information Assurance Partnership). This will help ensure standardized information protection and defense components are available which meet their intended security goals.

[6] Mission critical could include those systems that handle information vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified, sensitive, or unclassified information).

Mission support could include those systems that handle information important to the support of deployed and contingency forces. Information on these systems must be accurate, but can sustain minimal delays without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

Administrative could include those systems that handle information which is necessary for the conduct of day-to-day business, but do not materially affect support to deployed or contingency forces in the short term (may be classified but is usually sensitive or unclassified). It is recognized that this information may be recreated if the need arises.

7. Although this report has thus far focused primarily on network defense, Joint Pub 3-13 defines information warfare more broadly, to include electronic warfare (EW). In this regard, the task force recommends that DoD recapture its comparative lead in EW, which has eroded over the years.

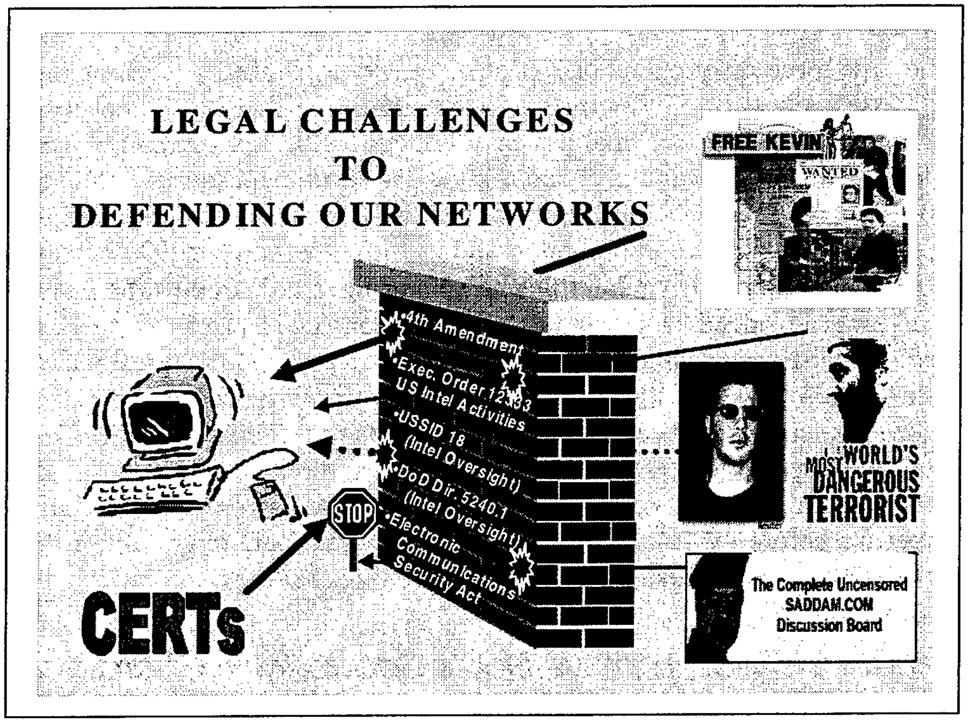
   a) The proliferation of advanced red/gray surface-to-air missile systems (such as the Russian SA-10), the modification of older Soviet systems to enhance their performance, and the introduction of innovative tactics using these systems have combined to increase the threat faced by U.S. aircrews. At the same time, the United States has reduced its ability to cope with this threat for several reasons. First, the United States has retired electronic combat assets such as the F-111 and the F-4G. Second, intelligence collection has focused on operational electronic intelligence (ELINT) in support of deployed forces at the expense of technical ELINT in support of electronic warfare. Third, personnel with EW experience have left the Services in large numbers. Fourth, DoD has fewer live-fly training events for its aircrews where they can operate in a realistic electronic combat environment (such as the Air Force's GREEN FLAG exercises).

   b) The task force recommends DoD place renewed emphasis on the entire chain of processes related to EW, from the acquisition of pulse and signal level data via technical ELINT to the analysis of this data to the reprogramming process that allows U.S. forces to rapidly reconfigure EW equipment to meet emerging threats. To do this, some recapitalization of the analysis and processing infrastructure is needed (for example, computer systems from the early 1990s at organizations such as the National Air Intelligence Center have a difficult time processing and analyzing advanced radar signals). In addition, DoD needs to press ahead with realistic Distributed Mission Training (DMT) Systems which use validated threat data. Use of DMT allows linkage of an array of assets (e.g., intelligence collectors, surveillance aircraft, strike aircraft) to be linked together virtually and exercise against realistic, rapidly-changing threat scenarios – all without expending flying hours. Finally, DoD must take steps to recapture personnel expertise before the last of itsEW experts departs. DoD might also enlist the help of the Old Crows Industry Association with this challenge.

Recommendation Two: Improve DoD's Capability to Characterize Probes and Attacks on Information Systems

It is important to emphasize that computers don't attack computers, Rather, people use computers as a tool to attack other computers, targeting the information or the ability to use the computer for its intended purpose. While DoD elements have the capability to detect some attacks against their information systems (for example, attempts to intrude on the NIPRNET), their ability to characterize such attacks is limited. Even when a source can be identified, there remains the greater challenge of identifying and characterizing the human element conducting the attack. There are several factors, which constrain DoD ability to do this.

First, legal considerations often preclude computer network defense (CND) personnel from tracing an intruder's electronic signature or finger print back to its electronic point of origin. For example, if an intruder stages an attack through a U.S. Internet Service Provider (ISP), legal restrictions preclude CND personnel from tracing the attack back through that ISP. While such incidents can and often are turned over to law enforcement authorities, resolution – if it ever occurs – can take weeks or months. During this time, the organization under attack has no method of ascertaining the true nature and intent of the attack and therefore is unable to determine appropriate defensive measures. The only response measure available in real time is to block the offending IP address at the router or firewall allowing the perpetrator to continue through a different IP address. Due to laws protecting U.S. persons, it is more advantageous for an adversary to establish an ISP in the United States conduct attacks and be out of the country before being apprehended. The fact the United States also has the most robust infrastructure in the world for conducting an information warfare campaign also makes this a more lucrative alternative.



LEGAL CHALLENGES TO DEFENDING OUR NETWORKS

- 4th Amendment
- Exec. Order 12333 US Intel Activities
- USSID 18 (Intel Oversight)
- DoD Dir. 5240.1 (Intel Oversight)
- Electronic Communications Security Act

CERTs
STOP
FREE KEVIN
WANTED
WORLD'S MOST DANGEROUS TERRORIST
The Complete Uncensored SADDAM.COM Discussion Board

Figure 19. Legal Challenges

Second, there is a lack of interoperable databases that seamlessly connect all CND entities, and that link tactical with strategic events. For example, the Service's Computer Emergency Response Teams do not use the same databases. Similarly, databases for the DoD Indications and Warning System for Information Warfare (termed CYBERWATCH) are not linked with any databases that monitor day-to-day intrusions into DoD networks. The basic problem arises from the fact that CND is seen as an operational and communications issue, which has little linkage to the Intelligence Community and its mission of foreign intelligence. In at least one location (the Air Force CERT), "tactical" and "strategic" databases are indeed correlated, but the process is entirely manual. Similarly, the NSA's National Security Incident Response Center maintains intelligence and intrusion databases. All these efforts among analytical and CND operations need to be linked together in an automated, relational manner.

Third, CND efforts to date have resulted in defending against the least resourced threats (not sponsored by a structured organization or government). The bulk of detected intrusions into unclassified networks can be classified as hackers, private individuals who for a variety of reasons attempt to intrude into DoD networks. In effect, DoD is often faced with reacting to "cyber graffiti" – attacks which are a nuisance, but which may not intend real or widespread harm to our operations. In part, this is due to the fact that the intrusion detection systems (Automated Security Incident Measure System, Netranger, etc.) are signature-based. They detect only what they are programmed to detect and therefore will not detect a new and/or extremely sophisticated attack. By its very nature, signature-based technology is post-event driven. The net result is an inability to identify new or on-going events that circumvent the signature-based technology, thus creating the potential for an attack that is even more detrimental.

Fourth, DoD must recognize the indications and warning capability in the area of information attacks is rudimentary. The Intelligence Community has had neither the time nor the resources to expand collection programs. Sufficient data must be collected to characterize the human element and determine which adversaries would perform these types of attacks and their specific methodologies for executing the attacks. Current IW indications and warning capability is largely reactionary, based on near-real time or past events collected by intrusion detection sensors or identified by systems administrators. The intelligence community at large does not consider these resources to be a source for collection of raw intelligence data feeding the IW indications and warning system. Instead, they use it more for a validation source, i.e. "Did we detect a particular event?" rather than "Are we seeing an event and how does this affect the U.S. national security posture?"

To remedy the above, DoD should do the following:

- Aggressively seek legal authorities and permit the implementation of technical solutions to identify the electronic point of origin of probes and attacks against DoD information systems. The intent of this would allow information defense entities to determine the nature, origin, and intent of probes and attacks against DoD systems. For example, such legal authority would allow DoD entities to determine – to some degree – what IP address is the root cause of an attack or probe. In other words, is it a person in New York or is it a foreign organization that intelligence sources reveal is connected to a hostile government? If the IP address correlates to a U.S. person, then the situation can be turned over to law enforcement authorities, as is now the case. If the latter case, then the situation can be investigated through foreign intelligence authorities.
- Establish a set of pre-approved response options that allow the Services and DoD commands to immediately react to threatening probes and attacks to prevent loss of data or denial of service. For example, if a U.S. system is subject to repeated "ping" attacks over a certain period of time, authority would be granted to immediately deny service to the originating entity, while allowing traceback to the electronic point of origin.

- Direct the JTF-CND and the Intelligence Community to build interoperable databases that address the range of warning issues from the strategic to the operational to the tactical. This will allow correlation of on-going activity, entered into CERT databases, with longer-term trend data in national-level databases. This will require a somewhat new mindset among both the Intelligence Community and the CND community – the realization that strategic indicators can help focus tactical defense and that tactical information can verify and amplify strategic indicators. The Air Force model at San Antonio, correlating the CYBERWATCH program with intrusion databases maintained by the Air Force Information Warfare Center, is an example of the type of process required at the national level, albeit it in a far more relational and automated form.
- Designate U.S. Space Command's Combined Intelligence Center (CIC) as the focal point for the CYBERWATCH process. As the JTF-CND is transferred to U.S. Space Command, transferring the national indications and warning mission for IW to the CIC is a logical corollary. This will ensure that one organization (U.S. Space Command) has responsibility and authority for the entire IW defense problem, from strategic warning through tactical warning through attack characterization and response. In so doing, it will tie the "intelligence" part of IW more closely with the "operations" part of IW, thereby increasing both effectiveness and efficiency. As part of this process, CIC must specifically focus on defining an IW warning problem and detailing the collection requirements to feed the indicators to that warning problem.
- Direct key agencies in the Intelligence Community – DIA, NSA, CIA etc – to integrate IW collection elements into the established collection networks (HUMINT, MASINT, SIGINT, ELINT etc.) This will provide an integrated decision process and begin to move the problem away from the perception that "a computer is attacking the network" to "a person (who may be state-sponsored) is attacking the network."
- Task the JTF-CND to begin developing tools to detect "low and slow" network attacks (i.e., sophisticated attacks against our networks that can last for days or weeks). Current automated intrusion detection (ID) tools cannot detect these attacks in either real-time or batch analysis mode (i.e., manual post-event review of intrusion detection logs) because they are below the threshold of current ID tools. In addition, many ID tools are configured to ignore certain types of network traffic to reduce background noise; as a result, they do not register "low and slow" attacks hidden in this background. Because all IP networks are vulnerable to this type of attack (e.g., NIPRNET, SIPRNET, etc), more thorough and efficient data mining and analysis tools are needed. The JTF-CND with the help of NSA and DARPA, must research and implement various types of ID tools (e.g., network based, host-based, etc) that will be able to collect this data and analyze it automatically, thereby reducing reliance on current manual analysis to detect these "low and slow" attacks. These tools must employ the use of heuristic analysis presenting analytical probabilities based on current and historical events. The tools must be scaleable to meet the needs of a single system, a small or large network, a metropolitan network, or global enterprise network. The tools must integrate into a distributed environment to meet operational needs presenting data in both tactical and strategic formats with decision aids to assist commanders with understanding the risks to operations. These tools must also begin leveraging artificial intelligence that will move DoD beyond signature-based models

and into tools that will help information protection personnel identify relationships that have not been described to the system.

- Along with directing the development of new tools to detect sophisticated attacks, the JTF-CND must lead the development of tools that assist in the aggregation, analysis and visualization of current network activity. At present, much of the analysis dealing with network probes or attacks is manually analyzed. The Air Force statistics in Figure 20 depict the magnitude of the problem. These tools can display the aggregated input from new sensors and analytical systems, allowing analysts to immediately focus attention on areas that have the most anomalous activity. Such visualization tools will play a key role in the ability to perform indications and warning for information protection and defense.

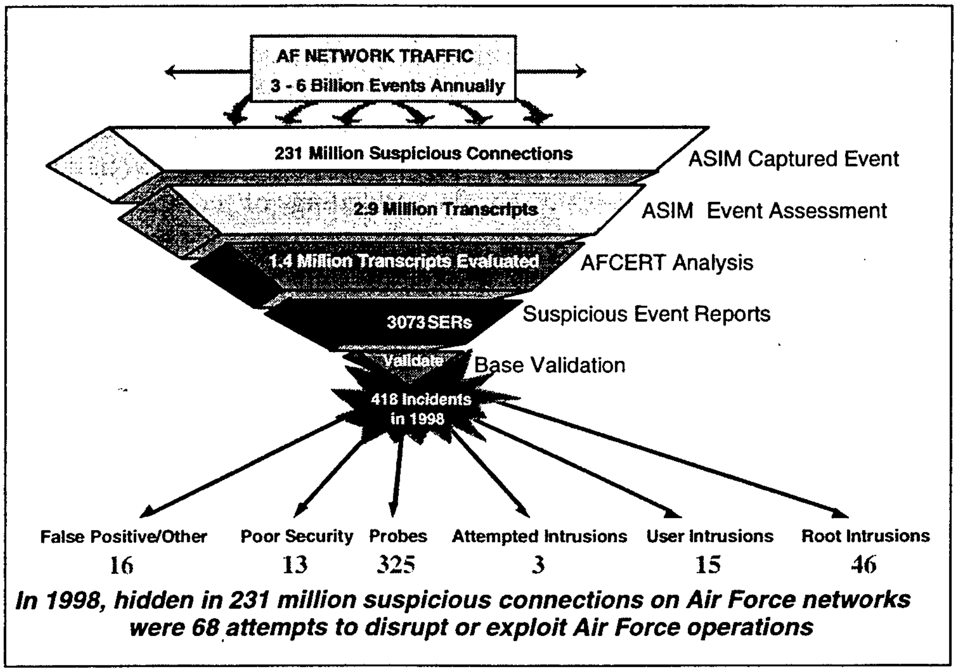


Figure 20. Complexity of Analyzing Network Activity

In addition to technical remedies, network defense personnel must ensure close coordination with counter-intelligence agencies, given the potential linkages between espionage and network probes or attacks.

Recommendation Three: Improve IW Training and Readiness

At present, IW covers a wide range of disciplines, ranging from communications-computer specialists to electronic warfare personnel to military deception planners. All these are "stovepipe" disciplines, in the sense that personnel often spend the bulk – if not the entirety – of their DoD careers in the same field. If DoD is to operationalize full-spectrum information operations – a necessary precursor to information superiority – then the Department needs to develop a cadre of "information operators" with knowledge of how all these disciplines interrelate. To do this, the task force recommends DoD do the following:

- Increase the awareness and training of all personnel involved in information operations. As part of this process, DoD agencies and the Services should develop education and training processes to baseline personnel in the broad array of all defensive IW functions and for selected personnel in offensive information operations. This means, for example, a training process where a selected cadre of information operators would receive a broad exposure to all disciplines of IW. In effect, an EW officer would be introduced to deception planning, while psychological operations personnel would gain an understanding of computer networks and information systems. Once trained, these information operators could populate CINC IW cells – covering all aspects of information attack and defense – to execute campaign planning in a much more synergistic way. On-the-job training and a rigorous certification program should be used to validate the schoolhouse process. For example, information infrastructure personnel would receive detailed hands-on training on cyber threats, vulnerabilities and countermeasures, and proper use of system security capabilities. As part of this process, the Services must develop mechanisms to manage these information operators throughout their careers, so their expertise can remain current. Finally, DoD needs to reward information operators commensurate with their skills and the requirement for those skills. The rewards can be a combination of incentives – larger enlistment bonuses, increased reenlistment and civilian pay bonuses, special schooling – that would cause these personnel to remain in government service.
- Develop a process that balances security versus operational requirements. The present system of Information Conditions (INFOCON) is a good start to addressing the problem of a DoD-wide response to information attacks. However, there is no established procedure for determining at what point a particular INFOCON level begins to impact command and control and other operational factors. Additionally, because information is the thread that crosses all threat boundaries, efforts need to be taken to define the relationship between DEFCONs, THREATCONs, WATCHCONs and the INFOCON threat levels. The series of exercises conducted by the Third Fleet, which determines the impact of various INFOCON levels in a benign training environment, is an example of the processes that DoD and the services need to institute.
- As part of this process, DoD should direct the Services and CINCs to practice and exercise operating in a degraded information environment. During the Cold War, the U.S. armed forces faced a serious threat from Soviet Radio Electronic Combat (REC)

units. As a result, the Services developed exercises in which U.S. participants were subjected to the same type of electronic attacks they might encounter from Soviet REC units. There is no corollary to this process in the current information realm. While DoD has experimented with IW exercises, they were basically closed-loop operations. All DoD personnel need to understand that critical information services may be degraded in wartime (from something as innocuous as a "minimize imposed" on an INTELINK server due to excessive demand or to hostile denial of service across entire networks). While a rigorous IW attack could bring entire exercises to a standstill – resulting in "negative learning" – a more incremental process is needed. Factors like network degradation, information attack, and INFOCON implementation can be introduced into exercises in a gradual mode, increasing in intensity as personnel become more familiar with countermeasures from exercise to exercise.

- To raise the level of awareness of IW readiness, DoD should implement a process that makes IW readiness an issue for CINCs. This IW readiness should address not just network security, but all pillars of IW (both offensive and defensive counterinformation). While some of this is currently accomplished in separate functional areas (for example, ability to conduct EW operations), the current effort is not all-inclusive, nor is it tied together under the broader context of IW. For example, CINCs should report on their ability to execute psychological operations (PSYOPS) against potential threats in their region well before the initiation of a contingency action, and how a potential adversary's ability to use cyberspace for propaganda might impact U.S. operations. As part of this process, CINCs should assess and test resources and capabilities against potential missions and include the results in standardized readiness reports.
- To aid in the proper security-operational requirements balance from a network perspective, DoD needs to execute a department-wide risk management process, to include common certification and accreditation procedures.

Recommendation Four: Designate San Antonio as the Alternative Site for the JTF-CND and the CND Tool Test and Evaluator

At present, the JTF-CND has no formally designated alternate capability. While this is not a major problem today (given the major roles played by the Service CERTS), it will eventually create a single-point failure as the joint task force's (JTF) responsibilities and capabilities mature. To remedy this situation, the task force recommends DoD designate San Antonio as the JTF-CND Alternate Site due to its in-place resources, technical expertise, and joint connectivity. Assigning this mission to San Antonio would provide an on-line back up to the primary JTF (much like the Joint Intelligence Centers have a back-up role for each other in an emergency). Equally important, San Antonio could become the prototype center in which new capabilities are tested and integrated prior to insertion into the primary JTF structure. This important function would ensure that primary CND and indications and warning functions could focus on the truly critical issue of keeping computers and communications operating as required.

San Antonio brings a variety of capabilities to the CND mission as a result of the organizational synergies present at Kelly Air Force Base.

The Joint Command and Control Warfare Center (JC^{2}WC) is the DoD organization chartered to provide full-spectrum information operations support to combatant commands. As such, the JC^{2}WC has standing CINC support teams that deploy to regional and functional CINCs during both exercises and crises. These teams provide linkage from San Antonio to the CINCs, and could therefore serve as linkage between the alternate JTF-CND site and the CINCs. In addition, with the resubordination of the JC^{2}WC to U.S. Space Command later this year, the tie between the collocated Air Force CERT and the JTF-CND's parent organization will become stronger.

As the Air Force Component of the JTF-CND, the Air Force CERT (AFCERT) is a part of the broader, day-to-day defense of U.S. military networks. The AFCERT has extensive experience defending Air Force networks, and represents the broadest and most mature CERT capability among all the Services. Providing back-up capability to the JTF-CND would therefore not pose great problems. Also, AFCERT has established ties with both the Federal Bureau of Investigation and the National Infrastructure Protection Center, broadening its coordination beyond just the Air Force network defense mission.

The Air Force Information Warfare Center (AFIWC) can bring a wide range of capabilities to bear in support of the computer network defense mission (e.g., modeling and simulation, the telephone system security assessment program, etc), computer network vulnerability assessments, and network security solution development. This includes the initiatives underway at the Air Force Information Warfare Battle Lab, also a part of AFIWC. The Air Force Battle Lab is already evaluating a number of state-of-the-art IW defense tools such as visualization systems, which makes it a logical contributor to the development of tools for the entire IW defense effort.

The Air Intelligence Agency's 690th Information Operations Squadron, located at Kelly Air Force Base, is an associate member of the DoD Indications and Warning System for IW. As such, it has been in the lead among the Services in developing the CYBERWATCH process. This function would underpin the alternate JTF-CND designation by providing a link between the CND mission and the Intelligence Community in San Antonio that would parallel the linkages between U.S. Space Command's Combined Intelligence Center and the JTF-CND. Also, the Air Force Information Operations Center at Kelly Air Force Base possesses redundant multi-level communications that can readily support an alternate JTF-CND.

Recommendation Five: Dramatically Improve the U.S. Information Warfare Defense Posture

As stated above, the most prolific – but not necessarily the most critical – threat is to unclassified networks. In order to limit the number of intrusions, the task force recommends the following steps be taken by 1 January 2001:

1. Direct that remote access to all DoD computers be via dynamic passwords, to be then followed by cryptographically based access control consistent with the DoD Public Key Infrastructure.
2. Direct that an acceptably robust encryption be used to protect all unclassified communications. This should conform to NIST Federal Information Processing standards, e.g. DES or 3xDES. This is analogous to the former communications process of "encrypt for transmission only," which was meant to complicate the

amount of data that a potential adversary had to screen. Taken together, these two steps will significantly improve the signal-to-noise ratio for intrusions and allow CND personnel to focus their efforts on priority threats.

- For the slightly longer term, the task force recommends several systemic improvements; these include:
- Developing and enforcing policies and procedures that facilitate coalition warfare and interoperability. An example is the ability to share encryption dynamically to permit secure communications and data interchange, while still protecting national security. Even relatively lower-grade cryptographic systems that protect information for the duration of its tactical value (several minutes to an hour) would be a vast improvement over the current process where encryption is seldom used.
- DoD agencies and the Services apply a common protection and defense technical framework, employing evaluated and validated security technology. This should guide the building of a genuine defense-in-depth approach to all aspects of the DoD information infrastructure (e.g., NIPRNET, Global Transportation Network, Global Command and Control System, Wireless, Combat Radio, and the Integrated Information Infrastructure, for example). This approach would include both robust perimeter defenses (such as intrusion detection devices) as well as layered defense techniques that protect hardware and software. The entire system must be designed with the insider threat in mind.
- Develop technologies, which allow dynamic assessment and reaction to the health of DoD's information technology infrastructure. By using techniques such as data mining, text mining, search engines, visualization tools, and computer identification, the Department can dramatically reduce the man-hours spent assessing system health and simultaneously improve defensive capability.

RADIO FREQUENCY SPECTRUM ALLOCATION FOR THE DOD

Background

Numerous attempts have been made during the past 3 years to reawaken senior-level DoD attention with respect to radio frequency spectrum (RFS) allocation processes and management of DoD's authorized RFS. In the United States, RFS is allocated, authorized, and/or licensed to various users through two principal methods: for Federal Government use, the National Telecommunications and Information Administration (NTIA), under the Department of Commerce, functions as the regulator and allocator of RFS with assigned oversight in the Office of Management and Budget. For RFS users other than the Federal Government, the Federal Communications Commission (FCC), through its Wireless Telecommunications Bureau, handles all domestic wireless telecommunications programs and policies, except those involving satellite communications or broadcasting, including licensing, enforcement, and regulatory functions. Wireless communications services include cellular telephone, paging, personal communications services, public safety, and other commercial and private radio services. The Bureau also is responsible for implementing the competitive bidding authority for spectrum auctions, given to the Commission by the 1993 Omnibus Budget Reconciliation Act.

DoD has a number of RFS regulatory measures in place providing policy, planning assignments, and programming responsibilities. Over the last 3 years, the Department has been implementing business process re-engineering initiatives under the umbrella of the Defense Reform Initiative (DRI). Many of the initiatives documented in the DRI resulted in the promulgation of directives – one of which was DRI Directive (DRID) 31. DRID 31 directed a fundamental re-engineering of the procedures, practices, and processes associated with DoD RFS allocation, management, analysis, and R&D. DRID 31 was followed closely by decisions promulgated in Program Budget Decision 082. The combined effect of these policy directives has been modestly effective in reawkening senior-level attention to RFS matters affecting military use of spectrum – both domestically as well as internationally.

In May 1999, the USD(A&T) requested the Defense Science Board Summer Study '99 task force on Information Superiority to assess the impact of these numerous policy, organizational, and procedural changes brought about by the various directives cited above. The purpose of this section of the DSB 1999 Summer Study final report is to provide this assessment albeit a cursory, very preliminary overview. A follow-on assessment will be undertaken by a dedicated DSB task force that will begin its work in the fall of 1999.

Overview

A member of the information superiority task force assessed the present status of RFS allocation and management in the DoD. This preliminary assessment revealed that much improvement has been made in areas such as clarifying specific functional responsibilities, identifying, allocating and realigning new resources, assigning new functional responsibilities, and heightening senior-level awareness and insight with respect to RFS issues – both domestic and international.

However, there are residual, legacy attributes and cultures within the previous spectrum management community which continue to hinder proactive, senior-level engagement in the decision making process for RFS issues as well as a much-needed advocacy process. As never before, private sector demands for access to RFS are increasing at an exponential rate – both in the context of U.S. domestic consumption and well as international. For U.S. military force operations, an ever increasing dependence on access to previously allocated portions of the RFS is at great risk in this now market-driven competition for access. Senior-level engagement and direct process involvement is mandatory if DoD RFS access is to be maintained at present levels or adjudicated as necessary to meet competing market-driven and politically motivated RFS access demands. The fact that U.S. law directs RFS to be sold at auction has awkened renewed interest in spectrum already allocated to Federal Government use by the NTIA; furthermore, other countries have discovered, due to U.S. actions, that spectrum access over which they have sovereign rights has a monetary value far in excess of other natural resources.

Though DoD conducts international, military-to-military negotiations for RFS access, these negotiations are being less and less forthcoming due to the political reality that RFS has great monetary value and for reasons that countries are, themselves, deploying new wireless technologies creating their own demand for in-country spectrum – in direct competition with their military establishments.

Further, as potential coalition partners, present allies, and others with whom the United States has military-to-military relations are learning very rapidly, newly deployed RFS technology systems will have enormous potential for frequency fratricide with military systems unless through analysis, modeling, and simulation are undertaken prior to granting U.S. military access to foreign RFS. Thus, the days of "easy access" and assumed availability of RFS on the part of the U.S. military are a bygone era.

As new wireless technologies are deployed around the world, increasing demand for access to the RFS, the U.S. military will be under ever increasing pressure to re-negotiate foreign access and will experience great difficulty negotiating for new access in this finite resource environment. It is the task force's preliminary assessment, given all the recent, productive process re-engineering efforts undertaken by the DoD over the past 3 years, that much remains to be done if the United States is going to maintain RFS access – either domestically, internationally, or both.

First, and perhaps foremost, is developing a National RF Spectrum Strategy. The RFS is, indeed, a finite resource; furthermore, depending on the specific wireless application, there are specific areas within the RFS whereby such applications must reside for reasons of operating efficiency, propagation anomalies, bandwidth needed, threshold noise levels, and more. ***The United States is the only nation that does not have a National RF Spectrum Strategy.*** As a result, in the inner workings of U.S. government, the United States lacks formalized guiding principles and associated policies that could be the underpinnings of such a Strategy.

Though DoD is but one federal department having RFS access requirements, its is clearly the department with the greatest demand and usage statistics. Therefore, it is suggested that DoD take an advocacy position within the National Security Council (NSC) to obtain a consensus for producing such a Strategy and assigning the task to the NSC staff. Present U.S. policy places the Office of Management and Budget in an oversight role with respect to the federal government RFS management matters, and it is not intended that this responsibility be shifted or altered at this time. However, the ever increasing domestic and international private sector demand for RFS is of such importance to future U.S. national security that the NSC is the most appropriate body to take on the creation of such a strategic plan and program. The National Strategy should incorporate both domestic as well as international "guiding principles" and policies for private sector, public safety, as well as federal government RFS requirements. ***The Strategy ought to provide a spectrum use vision, policies for implementing spectrum management processes, adjudication processes when competing demands can not be resolved at departmental or agency levels, negotiating principles and strategies, planned evolution policies incorporating requirements for an understanding of evolving technologies, and efficient spectrum use strategies for both the private and government sectors, along with other matters such as security-use policies, research & development policies, and guidance for the U.S. commercial sector as well as for federal government users, etc.***

Regardless of what is in such a strategy, the fact that the nation does not have an RFS strategy document makes diplomatic maneuvering within international bodies – such as the United Nation's, International Telecommunications Union (ITU) – difficult if not almost impossible. Each voting member of the ITU (having one vote) presents its requirements for spectrum access, makes deals inside this international body, builds coalitions supporting positions (often times contrary to U.S. objectives, such as the continuing international struggle over GPS spectrum access), and develops self-serving relationships across national borders in efforts to thwart favorable support for U.S. agenda items at various World Radio Communication Conferences (WRCs). The bottom line is that the United States is engaged in an international battle for spectrum access without a unifying strategy, top-line plan, unifying political consensus, and follow-on support or vision.

Within DoD, the same is true even though there are circulating drafts of spectrum management "vision" documents and the beginnings of a department "strategic plan." Without the unifying national strategy as an underpinning to these documents, they are liable to be seen as irrelevant outside the immediacy of DoD.

Though DoD personnel in the Office of the Secretary of Defense who are accountable for spectrum management matters have established excellent working relationships at NTIA and the FCC; none-the-less they are faced with an irreconcilable dilemma in that the FCC works for the Congress, not the Executive Branch, and therefore has to march to a "different drummer." Of concern noted during the task force assessment was the fact that DoD's most senior person representing the Department in RFS matters on a daily basis was not at an appropriate level to deal with interagency counterparts and certainly is not seen as being at a sufficiently high enough level to effect policies by the international community. Though measures taken to improve overall DoD RFS management are proving effective, the ASD(C^3I), Spectrum Management Office should be elevated to the level of a Deputy Assistant Secretary of Defense. At this level, the person occupying this position would be seen as having significantly more political impact and representational credibility than at present.

Conclusion

There are a number of other recommendations that will be considered by the new DSB task force being established in the fall of 1999. It is important to remind the reader once again that the discussion points raised in this report are a result of a cursory and preliminary look at the issues and challenges facing DoD at the turn of the new millenium.

There is no doubt, based on this brief assessment, there is a compelling need for much greater DoD attention to RFS allocation, management, access negotiation processes, and resultant process involvement at DoD's most senior levels. DoD's present investment in infrastructure using the RFS is well over $100 billion involving more than 800,000 systems. The present market value of those segments of the RFS wherein DoD has "primary" access, given the ever-increasing private sector demand for more spectrum access, is valued at more than $200 billion. With a finite resource at stake and DoD's present as well as expanding appetite for spectrum access unabated, clearly DoD's senior management must engage in a proactive role to insure the Department uses its allocated resources in the best interests of the nation.

C^{4}ISR AS A SYSTEM

R&D AND ACQUISITION STRATEGY

Overview

THE PROBLEM

The fundamental problem is that no one looks at the composite C^{4}ISR system as a system.

Currently, joint C^{4}ISR component systems do not work together well as a system. They are only assembled when a crisis arises, and hard-working people make the components work. There are few, if any, feedback processes in existence today that can lead to permanent improvement between crises. Information technology is evolving rapidly, more rapidly even than DoD can apply it. Rather, C^{4}ISR is seen as a collection of components or subsystems provided by many different organizations, at different times, and often with different design goals.

ONE SOLUTION

The suggested solution is to recognize that joint C^{4}ISR is not a collection of independent things, but a system, a very complex Joint Military Information System (JMIS).

As an analogy, an airplane can be thought of as a system, not as a collection of components. An airplane as a thing that works or does not, has desirable characteristics or does not, is easy to modify and improve or is not. There is a budget for an airplane or there is not. The tail cannot be left off and still have an airplane.

The JMIS should be considered in the same way. If the JMIS is not treated as a system, it will not work as a system. If it is not tested under the conditions in which it is supposed to work, it won't work under those conditions. If resources are not provided to fix problems, then they won't be fixed.

Treat the JMIS as a System

MAKE SOMEONE RESPONSIBLE FOR THE JMIS AS A SYSTEM

There is no mechanism today for designing and managing the JMIS. Progress is made primarily by various ad hoc arrangements, committees, integrated process teams, designated groups, and oversight organizations, each with responsibilities but with neither the authority nor the resources needed to carry them out. The decision about many important elements of the JMIS should not be left to different people scattered throughout DoD with only their own opinion about the system to guide them. Someone has to have the responsibility and authority for designing, testing, continuously operating, and upgrading the system as a system.

In the opinion of this task force, the Secretary of Defense should assign this responsibility to the Chairman of the Joint Chiefs of Staff (CJCS).

- The CJCS already has the job of assembling the forces provided, trained, and equipped by the Services
- The CJCS provides a unique oversight role and interface function to the Secretary for the warfighting CINCs who actually fight the forces when needed
- Only the CJCS and the CINCs can call together the forces needed for joint tests and evaluation (JT&E) exercises
- All other parties have component responsibilities and cannot be assigned the joint task without conflicts

This is a new job – all other elements of the DoD retain their existing roles. Hence, while the CJCS has the responsibility and is accountable for results, the CJCS must delegate responsibility for special problems to each of the Unified and Specified CINCs. Specifically, the United States Joint Forces Command might reasonably be given responsibility for the common C^4ISR system that is deployed with the forces as they are assigned to supported CINCs. The CJCS should give other CINCs the responsibility for solving their unique problems, which they must address using the common system, the standard architecture and interfaces.

ENGINEER THE JMIS AS A SYSTEM

Creating a system design for such a large and diverse system as a C^4ISR Global System is a difficult task, technically, politically, and bureaucratically. In fact, attempting to build a top-down design with a top-down design organization may not even be a good idea. Because of this, most – perhaps all – such large complex systems are not designed from the top down, but rather evolve gradually from the bottom up under pressures from their users, similar to the way the Internet is evolving. Communications and transportation infrastructures, even cities themselves, are created in this way.

Even if systems evolve from the bottom up, systems needs standards, building codes, and someone doing system planning, if the system is to evolve efficiently. The Internet, for example, perhaps the archetype bottoms-up organization, has the Internet Engineering Task Force that performs this system engineering function.

These same ideas need to apply to the JMIS. What this means is that the CJCS and the CINCs need a system engineering organization to develop an architecture or overall system design. The organization should appoint an overall system architect and give that person adequate technical and operational resources. This architect should not be in one of the Services, since each Service already has major component responsibilities. The architect's responsibility would be to lay out an "open" system based on commercial standards rather than a detailed design. The open system has a common architecture with standard commercial interfaces so that the system itself can evolve easily through new components built to those standards under the evolutionary pressures of the realistic exercises. The heart of such a system is a flexible communications system, such as the Integrated Information Infrastructure discussed earlier in this section and in Volume I of the Summer Study report).

Test and Operate the JMIS as a System

One key challenge is to test the current system through exercises that resemble realistic military operations to the greatest extent possible. Unfortunately (or fortunately), the DoD is not always operating in its designed-for environment – war – like a communication system is. The DoD normally exists in peacetime modes, testing and training with occasional large exercises of subsets of the system, occasional police actions, or small-scale operations. But if DoD is to ensure information superiority across the full range of operations, including large-scale wartime operations, DoD has to exercise forces *and the information systems* in that way. DoD needs the equivalent of large-scale operations of the kinds for which they are developing the information systems.

The design of these exercises should be a critical element of system development. The exercises should not be a set of those conducted by components for normal training purposes. Rather, they should be explicitly designed to stress the JMIS as a system. Because the CINCs have the joint forces and are under the most pressure to be able to fight when needed, these exercises should be planned and carried out by the joint using commands, supported by the Services and agencies. The CJCS and the CINCs must have adequate funding for these exercises. They should be able to "buy" the services of the Service component suppliers; otherwise, the component suppliers will find many reasons not to participate.

One critical aspect of the test and evaluation process is to establish performance metrics for the system. The JMIS, with the JT&E organization, should establish the right metrics and instrument the exercises accordingly.

Incorporate Transition Planning

Given focused responsibility, adequate funding, and an overall system design end-goal, the next step is to create a transition plan for moving from the existing polyglot system of information systems to the new design. Transition is a difficult problem using current processes. The system we have now exists, and new components are asked one by one to fit the vast world of legacy components. This places an enormous burden on a new component that is either so burdened that it cannot succeed or else forced to retreat into an inefficient but at least doable stovepipe of its own.

The JMIS is and always will be in existence. It changes by evolution, and not by replacement. Driven by continuous, realistic JT&E exercises, the JMIS should evolve in a direction which demonstrates new capabilities, procedures, and efficiencies. Guided by an overall architecture and standards, it should evolve efficiently.

FIX THE EXISTING SYSTEM

The DoD needs to make what they have now work better and to build on what they already have rather than starting over. In this context, DoD should improve the mechanism for rapidly fixing the troubles that exercises point out. The process should enable immediate fixes without being entangled with lengthy development processes.

The joint users are probably best at fixing and improving what they already have. Hence, they should be responsible for deciding how to fix problems they identify in joint tests and experiments. Along with this responsibility, they should have adequate resources to develop short-term (days or weeks) fixes.

DoD should enable continued innovations and create a process whereby everyone can do what they do now more effectively. Hence, the task force is not suggesting that the Services give up responsibility for their system components. Rather, the Services need to be aggressive and forward thinking. The "big money" will go through the Services as before. But they will have to "sell" their developments to the joint users. The Services will have to meet the standards set by the system architect. Through the CINC components, the Services should have a good handle on the problems JT&E exercises identify. The developing organizations should then go back to their parent organizations and be able to make more elaborate fixes and improvements but without the delays of the current process. The result should be a steady improvement of the existing JMIS.

LONGER-TERM IMPROVEMENTS

Proposals for longer-term improvements will come from many sources – from Services, development organizations, and contractors. The task force believes that the CINCs should play a larger role in influencing what the Services develop than is the case. But the CINCs should not be allowed to throttle new ideas in their cradles in order to spend money on near-term problems. Rather CINCs, through the Commander, Joint Forces Command, should more aggressively influence C^4ISR systems. CINC participation will automatically result in greater interest in and knowledge about joint needs and opportunities. More importantly, the Commander-in-Chief of the Joint Forces Command can provide a place where new ideas and devices can be tried out in limited operational experiments.

What we have in mind is a continuous ACTD process test-bed. ACTDs are designed to allow the war fighting community, i.e., users, to sponsor and then evaluate the utility and operational impact of novel, relatively mature technologies before committing to a formal acquisition program. ACTDs typically take 2-4 years to complete, and must be fully funded in the five-year budget. After the demonstration, operational units can continue using the hardware if appropriate, given the necessary support. Instead of the normal ACTDs, we envision a joint test-bed, owned and operated by the CINC Joint Forces Command, that is designed to focus on ideas for both the mid-term (the first few years past the FYDP) and especially the long-term (beyond 10 years).

By the long-term, most existing legacy systems will be obsolete and can be retired. Legacy systems that are still valuable should be modified to interoperate with the new system. This is better than distorting all the new things to fit the old. Major improvements between now and then should be designed to fit the new open system design. Over the period, the JMIS will gradually turn into what DoD really needs. The process of putting the system together and exercising it to make sure it works and that the users understand how to use it would continue at Joint Forces Command.

As at the present time, the Services and agencies will provide new information system components. But unlike today, the decisions about what the joint characteristics of these systems should be and whether in fact they are bought must be strongly influenced by the CINCs. Real power can be given to them by giving them strong influence over the final buy decisions. In addition, the process should require that the separate major component system designers and the overall JMIS architect sign off on the final buy decisions.

Implementation

CREATE A UNIFIED JMIS BUDGET LINE

The JMIS should have a system architecture, an operational and technical architercture, and a system budget. The ASD (C^3I) must plan and lobby for that budget. The JMIS budget would probably begin as an informal summation of the various component budgets for information systems, becoming more and more a part of the formal budget process as things proceed and the importance of a unified, joint, budget becomes widely understood.

The CJCS should be given the flexibility to influence modification of components. The budget should give the CJCS and the CINCs funding for JT&E exercises, the Joint Systems Engineering Organization (JSEO), and near term fixes. The CJCS and the CINCs should also have a high degree of influence on funding decisions for system components. Finally, changes to component systems must be possible without following lengthy acquisition processes prescribed for new systems in current acquisition regulations.

ESTABLISH THE JOINT SYSTEMS ENGINEERING OFFICE

The CJCS, and on his behalf the JFC, will need a Joint Systems Engineering Organization (JSEO) to help carry out the new system responsibilities. The JSEO should:

- Maintain a current system description
- Ensure that there is a system and technical architecture
- Establish and maintain interface standards
- Maintain system simulations, provided by component suppliers, as needed
- Provide planning, instrumentation, and analytical support to JT&E exercises, and define problems made apparent by the exercises
- Work with all DoD elements that have intersecting responsibilities for C^4ISR systems

To ensure that the JSEO has sufficient influence in the joint system, it should be led by a flag officer reporting directly to the CINC Joint Forces Command. That flag officer should have a lengthy tour of duty (nominal five-year appointment).

There should be a senior JMIS system engineer who oversees a CINC Joint Forces Command organization with substantial contractor support. The size of the contract effort should be fixed by the needs. Nominally, the task force suggests a size of the order on 300 professionals:

- About 100 in a central group at JFC to handle architecture, standards, outside interfaces, and common problems
- Another 100 professional engineers to assist with the common system JT&E exercises and fixes
- Another 100 engineers stationed at the CINCs as needed to help with their specific problems

This level of effort translates into a budget of some $50 million annually which is "cheap" compared to the sums spent to fix C^{4}ISR systems after major contingencies such as Desert Storm and Bosnia. Kosovo C^{4}ISR "fixes" follow soon.

Summary

To ensure information superiority, the DoD must begin to treat the JMIS as a system. Since there is apparently no mechanism for doing this within DoD, someone must be given responsibility for the JMIS and provided with the necessary resources.

The task force recommends that this new capability be assigned to CJCS, with responsibility for the core JMIS delegated to USJFC, that a Joint System Engineering Organization be established to provide the needed technical support, and that adequate funds be provided to support frequent JMIS tests and exercises and short-term fixes.

LOGISTICS

Introduction

Information is the backbone of modern logistics. In its most basic form, the logistics support challenge is primarily one of rapidly coupling "providers" to "users with needs" as directly as possible such that user downtime and total inventory are either minimized or eliminated entirely. The scope of DoD logistics operations is enormous and incredibly complex, having evolved to its present state over many decades from the bottom up, with little if any overall system engineering. Consequently, there are over 1000 different aging "logistics systems" in use, contributing to long cycle times and large inventories. Although the Department has made real progress in achieving interoperability between these systems at a technical level, most of the necessary business process changes to take advantage of this interoperability have not been made, resulting in continuing inefficiencies and higher than necessary costs.

The demands of *Joint Vision 2010* and advanced concepts such as the Rapid Reaction Force will require a massive overhaul of the Logistics information technololgy systems. Because the requirements for logistics information directly parallel those associated with warfighting operations, the new concept of *"Opergistics"* has been adopted from the Marine Corps and developed as part of this study, where the separation of logistics and operational functions is eliminated in favor of a unified, seamless approach. The following sections provide a more detailed description of the current situation, a view of the desired future, and some recommendations on how to get there. By the nature of this study, these tend to remain at a relatively high level, but nevertheless represent steps that, if taken, can make dramatic improvements for the future.

Current Status and Emerging Thrusts-1999 to 2002

Over the years, the logistics information systems have been developed in a largely independent manner by the Services and agencies, major commands, repair depots, and supporting defense contractors. Many thousands of different databases exist and are in use, and largely independent communications channels are used to transmit and distribute logistics information between the more than 1 million personnel who are actively engaged in this process. Over 1,000 aging (some over 30 years old) legacy systems of the military departments, United States Transportation Command (TRANSCOM) and the Defense Logistics Agency (DLA) support logistics operations. While these systems provide adequate support to current military operations, they are costly and time consuming to improve.

As an example, 10 years ago DoD's component organizations agreed to rules that would allow the automatic redistribution of assets among field organizations. However, because of the technical difficulty of making the needed software changes and weak management processes to ensure that changes are made, only now is that important process being implemented.

Improvements, such as fewer transactions to get materiel to the warfighter, more accurate forecasting of requirements, and more secure information are needed to enable logistics to respond to the dynamic environment of future military engagements. Concepts such as "near just-in-time spares" plus better use of the commercial/industrial infrastructure are required to reduce inventories and cut cycle time. Clearly, implementing these changes will require significant changes to business operations as well as the introduction of improved information technology systems.

Fortunately, significant efforts are underway within all the Services, DLA, and TRANSCOM to address many of these issues, although they remain largely stovepiped. The need for improvement is now widely recognized, and "thousands of flowers" are now blooming as individual thrusts are initiated to independently improve various segments in the process. Some of the more significant initiatives include:

- Army: Global Combat Support System (GCSS)-Army, Army Wholesale Logistics Modernization
- Navy: Navy Enterprise Resource Planning (ERP), MRP2, Shipyard Depot Modernization
- USMC: Integrated Logistics Capability, ATLASS II
- Air Force: GCSS-Air Force
- DLA: Business System Modernization, Fuel Automated System
- TRANSCOM: Global Transportation Network (GTN), TC AIMS II (Army is Executive Agent), GATES II, Worldwide Port System (WPS)

The aim of these initiatives is to improve the ability of the components to provide logistics support to combat operations. However, not all of the components have linked their programs to enterprise-wide plans for process improvement, and the Department lacks an operational architecture linking the component efforts with community services or objectives. An example of this is given by the implementation of GCSS – the Global Combat Support System. As originally envisioned, this was to be the support analog of the Global Command and Control System (GCCS) and was to provide a single interoperable system for all users. However, it has now evolved into individual approaches by each Service (e.g., GCSS-Army, GCSS-Air Force), in recognition of the substantial differences in legacy systems and fundamental support approaches that exist between the Services. Also, these component efforts and the need for joint GCSS capabilities are not yet synchronized.

Furthermore, component efforts are not all taking advantage of commercial software to rapidly adopt best commercial practices. Ones that are trying to adopt COTS applications are encountering hostile management processes and organizations unwilling to change their ways to adopt the practices embedded in software.

DEMONSTRATIONS AND PILOT PROGRAMS

There are also a large number of individual demonstration and pilot program initiatives within each Service, DARPA, and DLA. Although each taken by itself represents a worthwhile initiative, there is little cross-coupling between most of them, and equally troubling, there are often no concrete plans on how to migrate these demonstrations into main stream capabilities within a specific time scale and budget allocation. This can be illustrated by the following three key programs.

ADVANCED LOGISTICS PROGRAM

One of the more far reaching information technology initiatives is DARPA's Advanced Logistics Project (ALP), an R&D effort that promises advanced planning and execution capabilities in support of joint logistics operations. ALP is a five-year initiative aimed at gaining unprecedented control over the logistics pipeline. Its goal is to develop and demonstrate enabling technologies that will allow logistics and transportation assets to be deployed, tracked, refurbished, and re-deployed more efficiently. The Joint Staff/J4, DLA, and TRANSCOM are supporting the project. Briefly, its goals are:

- Automated Logistics Plan Generation – produce executable, level–5, time-phased force deployment database within 1 hour
- Real-Time Logistics Situation Assessment – identify plan deviations and re-plan within 30 minutes
- End-To-End Movement Control – minimize staging while globally optimizing lift resource usage across the spectrum of movement activities
- End-To-End Rapid Supply – continuously assess the demand and sourcing of materiel and supplies from DoD and commercial inventories

LOGISTICS ACTD

The Logistics Advanced Concept Technology Demonstration promises tools for displaying and manipulating logistics data from the component supply chains. It initially developed and demonstrated the innovative Log Anchor Desk which was deployed to Bosnia in 1996 but is no longer operational there. (Like many new ideas, there were some flaws in the concept, but rather than institute corrective measures and build on the good aspects of what was initiated, the entire concept was abandoned. Thus, little of lasting benefit remains from the effort and money expended)

A second capability – Joint Decision Support Tools, which provides web-based decision support for the logistician/warfighter – was demonstrated by ACOM/EUCOM in April 1999 and is to undergo further assessment on GCSS. For the future, Logistics ACTD Phase Integrated Information Infrastructure is to demonstrate real-time focused logistics by FY 2001.

JOINT TOTAL ASSET VISIBILITY

Joint Total Asset Visibility (JTAV) is another capability that proved its usefulness in Bosnia in 1996, providing for the first time an ability for viewers with access to track the location and status of specific joint component assets by use of tag, database, and related information technology. It represents a key tool in addressing both the in-transit and in-theater rapid materiel distribution and retrograde problems by fusing Component asset data for use by joint commanders.

Although each of these three capabilities is an important improvement, they remain stovepiped. For example, no plan connects these key capabilities so that the data provided by JTAV is focused on the requirements of ALP and the Logistics ACTD. Equally troubling, there is no plan or budget line to ensure that the capabilities promised by ALP and Logistics ACTD will be mainstreamed as operational systems.

ADDITIONAL PILOT PROGRAMS

Reducing the logistics footprint is an important aspect of focused logistics. Currently there are several ongoing simulation-based acquisition demonstrations of the ability to use advanced simulation techniques with intelligent models of a weapon system to improve system performance. However, these pilots are missing a fundamentally important objective. They do not yet include a funded requirement that these same weapon systems, in addition to being modernized, also be more agile, be designed to comply with modular open system concepts, and fail less – all of which would contribute significantly to force agility and lower total ownership cost.

SECURITY ISSUES AND RELATED ITEMS

The Defense Information Infrastructure/Common Operating Environment (DII/COE), while achieving interoperability among command and control applications, is oriented more toward developed software and less to the integration of COTS applications. The current direction of emerging security policy is to apply public key encryption techniques to build a Public Key Infrastructure (PKI). However, the PKI is currently oriented to human access – not the computer-to-computer communications that comprise the vast majority of logistics transactions (over 2.5 billion per year).

To ensure that logistics does not become the area of vulnerability exploited by information warfare adversaries, DoD needs to protect computer-to-computer communications as well. The Department also needs logistics-specific security policies to control aggregated logistics information and logistics information that is used in planning and conducting military operations.

[As an aside, DoD's approach to PKI implementation is focused on building it internally, rather than looking to existing commercial PKI service providers. Although COTS may be used in this effort, scalability of selected COTS has been raised as a challenge by defense officials. Scalability diminishes as an issue if the alternative of combining our non-classified PKI workload with the requirements of sensitive commercial traffic is considered.]

COMPUTING AND COMMUNICATIONS INFRASTRUCTURE

Logistics computing infrastructure is acquired inefficiently, as part of the acquisition of individual applications. Communications Access is inadequate during operations, as has been shown in all of our most recent engagements. Even though logistics traffic may be crucial to force projection progress, it receives low priority for bandwidth access.

GOVERNMENT – INDUSTRY INTERFACE

Until recently, the primary thrust for information transfer between industry and the government had been DoD-unique standards for electronic data interchange and non-standard formats for exchanging product or weapon system structural data. In a step forward, the Department now has emerging policy to require commercial transactions standards be used for electronic data interchange (EDI) and the establishment of central services for standards adoption and a reinvigorated data exchange rule adoption process. Still remaining, the Department has not yet determined the relationship between central data translation services and the JTAV program.

Programs such as the Joint Computer-Aided Acquisition and Logistics System (JCALS) and Joint Engineering Data Management Information and Control System (JEDMICS), among others, are used as internal stovepipes to access product data. It has now become apparent that it is essential to transform access to weapon system drawings and data away from this stovepiped legacy and instead to Web based access using standard generalized markup language (SGML) technology and central services for product data translation. This transformation is not yet part of a managed program which will ensure that quality product data is provided to the SBA function and used for daily configuration management.

Future Vision – 2006-2010

Although much good work is being done in many areas, it is clear that some radical top-level changes in approach are needed if the capabilities of *Joint Vision 2010* are to be accomplished and if the critically important reductions in cycle time and cost of the support tail are to be realized.

The following table illustrates the transition states for the key logistics modernization factors:

Logistics Information Architecture

KEY AREA	*CURRENT STATUS 1999*	*EMERGING STATUS 2002*	*FUTURE VIEW 2006-2010*
Decision Support	Stovepiped Decision Support	Reporting Using New Metrics	Unified "Opergistics " Focus---Management Data an Automatic Product of Operations
Acquisition Focus	Initial Operational Capability (IOC) Focused Acquisition	Total Ownership Cost Simulation Based Acquisition (SBA) Pilots	Reduced Logistics Demand & Simulation Based Lifecycle Management
Logistics Planning and Execution	Minimal Automated Support: Static-Rigid	Advanced Logistics Program (ALP) Log ACTD/JTAV	"Opergistics" & Simulation Based Lifecycle Management
Metrics	Functional and Sub-Optimal	Mission Oriented	Outcome Oriented
Component Supply Chain Systems	Numerous, Expensive and Time-consuming to Improve	Modernized but Costly and Change Still Difficult	Network-centric, Secure, COTS-based, Adaptable
Government Industry Interface	MILS & Limited Commercial EDI. Non-Standard Product Data Interchange	ANSI/EDIFACT Commercial EDI Web-based, Industry Standards for Product Data Exchange.	Standard Interface to Industry Enables Efficient Partnering
User Interface	Legacy System Unique	Modernized but Highly Vendor Unique Multiple Interactive Electronic Technical Manual (IETM)	Common User Interface
Information Infrastructure	Stovepiped: Vertically Integrated Inflexible Imbalanced	DII/COE: Mission Oriented More Secure C^2-Oriented Interoperability	Integrated Information Infrastructure: Secure, Adaptable Supports COTS Balanced Bandwidth Access

Transforming the "emerging" picture into this vision of the future requires recognition that "the probability of success is not independent of the speed of implementation." Only by focusing resources and putting agile management processes in place can the Department assure attainment of this vision. All of the recommendations that follow have this effect.

Recommendations

The primary logistics modernization challenge facing the DoD is essentially one of achieving focused and timely execution. There are few if any technical barriers, and no inventions are required – virtually all the needed techniques have already been proven in today's fast advancing commercial world.

Because of the enormity of the task and the large number of players involved, it is essential that OSD, the CJCS, the Service Chiefs, and CINCS jointly embrace, support, and provide sustained reinforcement to a common vision for this important area. The following recommended actions are offered as positive steps to facilitate this:

- Deputy Secretary of Defense and the CJCS issue Policy supporting primary attributes of future logistics modernization goals, reflecting CJCS doctrine, component joint combat support requirements, and best commercial practices (such as changing the process, not the commercial software), with associated time table for implementation
- USD(A&T) through the Deputy Under Secretary of Defense for Logsitics [DUSD(L)] lead a collaborative effort across DoD to develop "to-be" operational and system logistics architectures by 2000
- USD(A&T), through DUSD(L), in concert with the DoD Chief Information Officer and the logistics leaders of the Components, create a portfolio of community capabilities in accord with these architectures to include the following:
  - ➤ Simulation Based Acquisition
    - – Establish formal programs for simulation based acquisition (SBA) and selected capabilities from the Advanced Logistics Project
    - – Synchronize these programs so they use the same model of logistics operations, creating the Simulation Based Lifecycle Management approach
    - – Focus SBA on improving the agility and reliability of existing systems via modernization through spares and other upgrades
    - – Require program offices to use SBA in conjunction with integrated development environments linked by the product data mediation services mentioned below
    - – Examine ALP to identify those planning and execution capabilities which can be extracted and developed for immediate fielding
    - – Immediately Transition those portions of ALP to a joint program office led by a component executive agent and fund to field a worldwide capability for CINC J-4s
- Corporate Mediation Services for Product and Transaction Data
  - – Establish corporate data mediation services for product and transaction data that:
    - ▪ <u>Restructure and focus</u> initiatives such as JCALS, JEDMICS, JTAV, GCSS (from DISA), and
    - ▪ Rationalize them with existing capabilities such as those of the Defense Automatic Addressing Service Center (DAASC)

    - Ensure that these services:
        - Provide easy access to authoritative, quality data in component supply chains, and
        - Be focused on supporting validated requirements of Joint (such as SBLM) or inter-component automated applications
    - Through a combination of quality and accessible product/transaction data, achieve the goals of:
        - Effective configuration management of fielded systems, and
        - Getting the right part to the customer when it is needed

- Common Industry and User Interfaces
    - Establish joint and common industry/user interfaces to facilitate efficient partnering with industry for product support.
    - The industry interface should be thought of as a <u>commercial transaction set</u> which allows DoD officials to oversee the performance of their industry partners while also serving as a product data interface for sharing engineering information.
    - The common user interface would be a combination of standard integrated electronic technical manuals for maintenance access to product data, and standard browser conventions for access to component supply chains with a common look and feel, regardless of the source of supply.

- Logistics Decision Support
    - Establish and utilize logistics decision support to enable the logistics leadership of the components and joint community to measure progress toward agreed upon strategic goals for the support of military operations and for achieving commercial-strength efficiency.

- Component Initiatives and Roles
    - Each component should be responsible for developing its portions of the overall operational and system architectures and for modernizing its supply chain in accordance with them.
    - Supply chain modernization should employ *<u>Unmodified</u>* COTS application software wherever possible.

- Policy on COTS Software
    - Use of COTS application software is only feasible if components change their business processes to accommodate the software and not the reverse. In the commercial world, such an approach works only when supported actively by corporate leadership.
    - In DoD, policy from the Secretary of Defense that requires maximum use of commercial software, changing business processes to accommodate it, and

continuous, strong leadership support for process change would be the right top-level message.

- This policy from the Secretary should be augmented by a USD(A&T)/DoD Chief Information Officer review of the technical standards and management processes governing application software acquisition. This review should result in mediating barriers to successful COTS application implementation such as DII/COE rules on segmentation.
- A way to conduct this review would be to designate an emerging COTS logistics software acquisition as the model and develop new standards/procedures for that acquisition.

- Portfolio Management Approach
  - To ensure that limited resources are focused on needed change, the logistics community should implement portfolio management processes to govern all of the funds expended on logistics information technology.
  - Each component would have its own portfolio of supply chain applications but would follow its portfolio management processes with common attributes across DoD.
  - These processes should ensure that:
    - Funds expended on changes to existing systems are limited to ONLY those improvements that would NOT be more cost-effectively implemented via modernization programs.
    - Formal requirements for modernized component supply chains be minimized, limited to those dictated by either the functional requirements of joint combat operations or the technical requirements of good information management, such as:
      - Total asset visibility, networked architectures, security
      - Compliance with commercial transactions standards policy
      - No wholesale/retail barriers
      - Support for corporate performance metrics, management data generated automatically as a by-product of operations, and
      - Automatic receipt of materiel that closes all associated logistical and financial transactions

  - Demonstrations and prototypes, such as the Logistics ACTD, are "mainstreamed." That is, they are only undertaken if, when successful, one or more components will implement them in their supply chains.
  - Investments not justified by specific functional improvements are justified by measurable reductions in the time and cost of improvement generally.
  - Resources are focused on those investments which will achieve or enable the greatest improvement in logistics' contribution to combat operations or savings in the cost of logistics support.

- Investments in information infrastructure (computing environments and communications) are separate from investments in applications and justified by the aggregation of applications supported. These infrastructure investments comprise the Integrated Information Infrastructure portfolio.
- Opportunities for new joint applications, community services, or common applications are identified, the requirements validated, executive agents assigned, and products delivered under acquisition discipline.
- Expenditures result in an acceleration of logistics process improvement.

- Policy on Business Rules for Logistics Data Interchange
  - DUSD(L) should issue policies that result in reinvigorating the process for achieving agreements on the business rules governing the interchange of logistics data among DoD Components.
  - This policy should ensure that joint programs such as those included under Simulation Based Lifecycle Management are equal claimants in accessing data from Component supply chains.
  - This policy should also ensure that business rules agreed to by components are implemented expeditiously by setting forth expected schedule target guidelines.

- Policy on Modular Open Systems Approach
  - Deputy Secretary of Defense and VCJCS should issue policy mandating use of the modular open systems approach on all new and retrofit acquisition programs in order to address the diminishing manufacturing sources problem, reduce the logistics footprint, and facilitate Interoperability between systems. This should apply to all acquisition programs, not just information technology systems.

- Policy on Information Assurance
  - DUSD(L), in conjunction with the DoD Chief Information Officer, should issue policy on logistics information assurance. This policy should guide the levels of protection and investments required in the protection of logistics information.
  - Computer-to-computer communications must be secure. The policy should cover the procedures governing the granting of personnel access.
  - Similarly, this policy should guide the interaction between components and the joint logistics and operations communities to assure adequate priority is assigned to logistics traffic.
  - In acquiring security protection for unclassified information, DoD should consider acquiring commercial services as opposed to integrating or modifying commercial security products internally.
  - An approach which has the DoD as one customer of a commercial enterprise serving multiple corporate and government entities may provide needed protection more quickly than internal approaches and mitigate problems of scalability.

MEMBERSHIP

INFORMATION SUPERIORITY TASK FORCE

Co-Chairs:	Dr. Taylor Lawrence, Northrop Grumman
	Mr. Robert Nesbit, MITRE
Members:	Dr. Stan Alterman, Alterman Associates, Inc.
	Dr. Theodore Bially, Atlantic Aerospace and Electronics Corp
	Mr. Robert Everett, Consultant
	Mr. Bran Farren, Walt Disney Imagineering
	Dr. Michael Frankel, SRI International
	Mr. Charles Gandy, Consultant
	RADM Robert Gormley, USN (Ret), The Oceanus Company
	Dr. Anita Jones, University of Virginia
	Maj. Gen. Kenneth Israel, USAF (Ret), Burdeshaw Associates
	Honorable Noel Longuemare, Consultant
	Dr. Greg Poe, Logos Corporation
	Mr. Jeffrey Sands, MITRE
	Mr. Howard Schue, Technology Strategies & Alliances
	Mr. George Spix, Microsoft
	Mr. Vince Vitto, Draper Laboratory
	Dr. Dick Wishner, Consultant
	Mr. Owen Wormser, C3I ®
	Mr. Lawrence Wright, Booz-Allen & Hamilton
Government Advisors:	LTC(P) Stephen Broughall, USA, DISC4/ SAIS-AI
	Col Mike Fallon, USMC (Ret), General Dynamics
	Mr. Michael Fleming, NSA
	LtCol Tom Hardwick , USMCOUSD (policy)
	BrigGen Paul Lebras , USAF AIA/CV
	Maj Ed Loxterkamp , USAF HQ USAF/XOIRN
	RADM Martin Mayer , USN J-8
	Mr. Mike Powell, USAIC&FH
	CMD James P. Steele , USN J-6,
	Maj Clinton Wadsworth USMC, MCCDC
Executive Secretary:	Dr. William Jeffrey, DARPA
DSB Military Rep:	Major Tony Yang, USAF, Defense Science Board
Support:	Mr. David Greinke, Strategic Analysis, Inc.

PART III. DEFENSE TECHNOLOGY STRATEGY AND MANAGEMENT

EXECUTIVE SUMMARY

INTRODUCTION

The Defense Technology Strategy and Management task force of the Defense Science Board (DSB) 1999 Summer Study was charged with identifying technologies that could improve the capabilities of the U.S. military forces by an order of magnitude within the next 10 to 25 years. The task force was also charged with recommending how to improve the management and execution of the Department of Defense (DoD) and Military Service Science and Technology programs, as well as the DoD acquisition system.

STRATEGY

The task force examined existing and potential national security challenges that U.S. forces might have to meet. In light of these challenges, the task force concluded that the most important capabilities that U.S. forces lack are:

- Response to engineered biological threats
- Real-time surveillance and targeting, especially of hidden and moving targets
- Rapid projection of dominant U.S. / coalition military forces

The task force then examined which technology developments are central to achieving these vital new capabilities. Several were identified and are discussed next. However, the task force observed that what is central to obtaining the new military capabilities identified above is the interdisciplinary development of these technologies. It further judged that pursuit of such technology combinations could be valuable to focus technology developments. These were identified as "Grand Challenge" military capabilities and, as such, are the appropriate focus for future DoD science and technology (S&T) programs as well as for acquisition programs. Four such Grand Challenge capabilities are discussed in the report and are summarized below.

Finally, the task force examined the vital issue of rejuvenating the management and execution of DoD S&T programs and the problem of transitioning new technology into advanced military capabilities.

CRITICAL TECHNOLOGIES

Four technology areas were identified by the task force as critical DoD. They were:

Biotechnology: Rapid detection systems for chemical and biological agents; new treatments for victims of biological attack, biological digital logic and memories; synthesized biological systems.

Information technology: Advanced algorithms for detection, identification and targeting of concealed, buried, and moving targets; cognitive decision aids for commanders; advanced optical and covert communications; secure network technology; high-resolution displays.

Microsystems: microelectromechanical (MEMS) components, devices and systems; ultra-high-speed optical logic and memories; nano-scale integrated integrated devices; mini and micro-robotic technology; quantum computation and devices.

Energy and materials: High-energy-density fuels, explosives, and propellants; super-strength materials; advanced energy-conversion systems.

While commercial sector investments in all of these technologies substantially exceed DoD's investments, most of the civil investments have a time horizon of only a few years. As a result, DoD needs to focus on the long term, more speculative aspects of these technology areas.

More importantly, DoD needs to focus on the interdisciplinary *combinations* of these technologies as the task force believes that it is in this area that the truly revolutionary advances in military capabilities will take place.

Grand Challenges

The task force identified four new military capabilities that incorporate the above technologies to yield the needed order of magnitude or more increases in the capability of future U.S. military forces. These capabilities have been put forth as Grand Challenges for the DoD S&T and acquisition programs and are summarized below.

Bioshield - Response to a Major Threat to the United States

In the 1990 Gulf War, concerns were raised about the potential impact of a biological warfare attack on U.S. forces in the field or upon civilians in the homeland. In the intervening years, further study has indicated that this threat is more serious than originally imagined.

Since the Gulf War, some technological progress has been made on the problem of detecting biological attacks, as well as the problems of protecting troops and treating exposed individuals. However, citizens and troops remain very vulnerable.

The task force proposes a major program to focus on this critical problem. The program would be composed of the following efforts:

- Wide-area detection systems, involving distributed sensors and warning networks which could warn of and identify biological agents within less than a minute.
- Rapid detection of biological-agent infections in humans in the approximately one minute.
- Development and production of broad-spectrum vaccines and antibiotics for treating broad classes of biological agents.

- Detection of biological-agent research, production, and stockpiles in potential aggressor nations.

To attack this serious threat to U.S. national security this task force recommends:

- Funding in this area should be increased from the current level of $1 billion per year to the order of $2 billion per year.
- Consideration be given to creating a DARPA-like organization outside of the existing military biological organizations. The staff of this organization should be drawn from the best experts in biological firms and academia.
- Support for this very important program can be sought from the biological industry. This will probably require extensive exemptions from the Federal Acquisitions Regulations because these firms are engaged in intense competition and are not likely to reveal their cost structures or many other aspects of their operations.

This DSB task force as well as a number other studies, including the recent Deutch-Spector Commission, see biological warfare as perhaps the most serious threat to the United States as it enters the 21st century. The current efforts to counter this major threat are simply not adequate when compared with the impact of such an attack.

No Place to Hide - Ubiqitous Microsensors

Recent experience in Bosnia and Kosovo has shown the capabilities of adaptive enemies and has indicated the extreme difficulty of remotely targeting military vehicles and forces hidden under foliage, in buildings, and in underground facilities. Such targets have traditionally been dealt with by ground troops who often suffer losses in the process.

To meet this Grand Challenge the task force envisions the creation of a new class of surveillance capability, involving the use of as many as 100,000 to 1,000,000 micro-sensors distributed over a theater of operations, but concentrated in critical target areas. These micro-sensors would be able to provide continuous surveillance of concealed and moving targets with an array of different detectors, such as biological, chemical, optical imaging, acoustic, seismic, and electromagnetic. Advanced energy systems coupled with covert communications would transmit data to overhead receiving systems for processing into detection, identification and target data.

Some of the micro-sensors would have ground or air mobility to allow advantageous placement and observation. It is anticipated that some degree of robot intelligence could be incorporated to enable the micro-sensors to investigate concealed targets on their own.

This class of surveillance and targeting system, together with greatly improved versions of the more conventional remote air- and space-based sensors, should allow future U.S. military forces to find, identify, and target aggressor military equipment and forces that are concealed under foliage, in buildings, and perhaps in underground facilities. In addition, such a sensor capability should allow identification and targeting of moving targets, even under foliage.

A joint Service program should be established, focusing on advancing technology in a variety of ultra-small sensing devices, micro-high-energy density technology, micro-robotics and air vehicles, covert communications technology, ultra-small data processors and memories and the integration of these into very small, low cost systems. While civilian technology development is proceeding in some of these areas, most of it is focused on the near term. These technologies would be combined to demonstrate initial military capabilities.

Funding of the order of $500 million per year is recommended.

Fast Forward - *Rapid Global Power Projection*

As discussed in detail in Volume I of the Summer Study report, the deployment speeds of U.S. forces are grossly inadequate compared with the need to quickly counter aggression.

In order to vastly increase the mobility of our military forces, especially ground forces, new approaches are needed. Much can be accomplished by redesign of the forces, but technological advances can offer further major gains. Fortunately, over the next 10-20 years, such an advance is possible. The twin keys to such an advance lie in three technologies:

- Ultra-high-strength materials
- High-energy-density fuel, propellants, and explosives
- Robotics

Utilizing possible advances in these technologies can result in aircraft that can fly several times as far and engage in combat many times longer. Also, weapon sizes and equipment weights can be reduced many times. Table 1 indicates the possibilities of higher strength materials:

Material	**Strength (in lbs/square inch)**
Mild Steel	20,000
High strength steel	150,000 - 300,000
Graphite composites	500,000 - 1 million
Carbon nanotube composite	2-10 million
Pure carbon nanotubes	25 million

Table 1: High Strength Materials

Since most equipment is constructed of mild steel, short-term advances using graphite composites could reduce weight, without sacrificing strength, by a factor of 10. The really astounding possibility, however lies with carbon nanotubes, which could reduce weight by 100-fold or more without sacrificing strength.

Today most military systems, with the exception of nuclear powered ships and submarines, use petroleum fuels that yield about 20,000 BTU per pound when burned with air. Table 2 indicates current capabilities and some future possibilities:

Material		Energy Density	
		BTU per lb	**Megajouls per KG**
Fuels	Petroleum with air (current)	18,600	43
	Hydrogen with air	51,600	120
Propellants	Hydrogen-Oxygen (current)	460 seconds Isp	
	Metastable N2-H2	500-1,000 seconds Isp	
Explosives	HMX (current)	2,600	6
	Metastable H2-N2	8,600-40,000	20-94

Table 2: Fuels, Propellants and Explosives

Because of the great importance of reducing deployment times and sustainment demands of U.S. military forces an intensive S&T and demonstration program is recommended at approximately the following levels of S&T investment:

• Super-strong materials	$50 million per year
• High-energy-density materials	$50 million per year

Follow-on product demonstration programs involving long-range aircraft, new lightweight weapons, rocket propulsion systems, and lightweight combat vehicles would require a minimum of $100 million per year. These programs would have to be pursued for a minimum of 10 years before these new materials would be ready for inclusion in acquisition programs.

<u>"Cognitive C^4"</u> *– Information and Command Systems with Near Human Capabilities*

The Summer Study identified improved C^{4}ISR, information superiority, and decision superiority as essential ingredients of future U.S. forces. Decision superiority in particular, requires semi-automated and automated information technologies to radically speed assimilation, decision-making, and decision-execution. Even if the combination of distributed surface sensors and satellite- and unmanned aerial vehicle (UAV)-based sensors can find hidden and moving targets, there remains the problem of understanding and acting on the resulting huge flow of data. This Grand Challenge focuses on this problem.

The principal tool for addressing this challenge will be the rapid increase in the capability of computers, along with developments in algorithms for recognition, information extraction, decision aids, course of action analysis, dissemination, and decision execution. At the more basic technology levels, agent-based software, human-computer interfaces, and other technologies play a major role. Over the past century, the cost of computation capacity has been declining by a factor of two every 18 months. This trend was observed by Moore and is the basis of his law. There is no reason to expect that this trend will not continue for many years into the 21st century. If so, it is reasonable to expect that within 20 to 25 years, computer capacity will have grown by 100,000-to-1,000,000 times. This means that modest-sized computers will approach or begin to match the capabilities of the human brain.

Civilian technology development will sustain short-term advances in computer capacity and algorithms; it will be necessary for DoD and the Services to address longer-term technology needs and uniquely military technology needs. As a result, the following are the needed foci of this Grand Challenge:

- New classes of computation technology; present CMOS technology cannot be the basis of an increase in speed of several orders of magnitude
- Effective automatic target recognition algorithms or, more generally, approaches to turn data into information
- Decision aids with near human capability for use by field commanders
- Anti-jam, higher accuracy navigation to provide the essential "common grid"
- Long-range communications for troops on the move
- Secure and reliable computer networks
- Data presentation systems that are matched to the needs of troops in the field
- Human-computer interfaces that are much more user friendly

A comprehensive and coordinated program should be organized at the level of the Office of the Secretary of Defense (OSD) to develop the technologies needed by future Cognitive C^4 systems. The Defense Advanced Research Projects Agency (DARPA) is a possible focus for such a program. Annual funding should be the order of $700 million per year.

S&T AND ACQUISITION MANAGEMENT AND INVESTMENT STRATEGY

The DoD system of technology development and system acquisition has progressed but still retains much of the character of the later days of the Cold War. This approach is no longer suited to cope with the critical national defense problems facing the United States in the 21st century. As the country moves into the new century, many new circumstances confront DoD:

- The current DoD/Service S&T laboratory system tends to focus on the weapon systems of the 20th century and not on the technologies of the 21st – such as molecular biology, intelligent information systems, new computation paradigms such as quantum systems, and other leading edge technologies
- Civilian technology in many areas has outstripped the DoD
- Globalization of industry and technology permits rogue nations to access leading defense technology and equipment
- Competition for leading technical staff from the expanding private sector technology developments has left the Defense Department and Service laboratories with great difficulty in attracting qualified staff because of the severe constraints of the Civil Service Personnel System

- Transition of technology advances from civil developments and the DoD S&T programs into acquisition programs is very difficult because of current contracting and acquisition regulations

This task force recommends the following:

- At least one third of the DoD S&T program should be focused by Grand Challenge programs of the type described above and which provide technology that offers order of magnitude gains in military capabilities. In addition to the programs described, there may be other Grand Challenge efforts that are important for DoD to pursue in the 21st century. The selection of Grand Challenges programs should be made by senior OSD research and development (R&D) management in consultation with the Services, Joint Staff and the "Futures CINC." The management of the Grand Challenge programs should be based on DARPA-like organizations operating at the OSD level.
- The funding recommended in this report for the four Grand Challenges is summarized in Table 3. This is not intended to be new funding but rather a shift in focus of current S&T funding:

Bioshield (additional funding)	$1,000 million per year
No Place to Hide	$500 million per year
Fast Forward	$200 million per year
Cognitive C^4	$700 million per year
Total	**$2400 million per year**

Table 3: Recommended Grand Challenge Funding

- The S&T program should not attempt to compete with ongoing shorter-horizon civilian technology development programs. Instead, the program should take advantage of these and be aimed at longer-term (5 to 20 years) technology developments which are not the focus of commercial research.
- In the future, the staffs of the Service laboratories and S&T Service management offices should be acquired from universities and their associated laboratories and from highly ranked industrial laboratories instead of from the Civil Service system. Modest terms of appointment (four to eight years) should be used to insure a constant flow of new ideas and to assure freedom to change directions consistent with the pace of technology.
- Promising technology successes should be better transitioned into military force capabilities. This should be encouraged through the use of enhanced Advanced Concept Technology Demonstration (ACTD) and similar programs, which have a second phase that provides initial funding for experimental forces and equipment in quantities large enough so that they could be used to augment the then conventional

forces responding to future contingencies. This much more rapid transition of technology into useful military capability is essential since our adversaries are generally more able than we in this transition and thus could enjoy serious military advantages in some areas.

SUMMARY RECOMMENDATIONS

The Under Secretary of Defense for Acquisition and Technology (USD(A&T)) should undertake the following:

- Initiate Grand Challenge technology efforts under the S&T Program utilizing at least one-third of the S&T Program funding
- Manage the Grand Challenge Programs using DARPA-like organizations staffed from the private sector, universities, and leading industrial laboratories
- Reinvigorate the Service laboratories by staffing them in the future with temporary assignments from universities and their laboratories, as well as from leading industrial laboratories
- Facilitate the transition of new S&T technology to military capabilities through the use of expanded scope ACTD programs, which produce initial combat capabilities involving both new equipment and assigned forces. The Joint Requirements Oversight Council (JROC) should participate in the establishment of these new combat capabilities

PREAMBLE

Since the end of World War II, technological advances have provided new, unique, and overwhelming capabilities for the military forces of the United States. These advances have primarily been technology pushes into DoD systems, often with DoD-unique objectives and interests, and typically developed by defense-sector industries. The overarching technologies of military relevance have been aerospace, information, nuclear, electronics, missile, and marine/undersea technologies. In these technology areas, evolution cycles and technology times were measured in years and decades, and the technologies were difficult and costly for our adversaries to develop or acquire. The capabilities that the United States derived from these technologies are unique and overwhelming.

Since the end of the Cold War, however, the technology landscape has changed – and the change is accelerating. The landscape for the next two decades differs from the technology landscape of the last two decades in five fundamental ways.

- Advances in most technology disciplines will increasingly be driven primarily by commercial interests
- The *pace* of advance in those technology areas that have military relevance is increasing
- The *types* of technologies that are militarily relevant are changing and increasing in number
- New capabilities and quantum jumps in old capabilities are increasingly occurring at the intersections of different technologies
- Turning technologies into military capabilities is governed less by who develops better technologies first and more by who has the better process of experimenting with and integrating technologies into systems

This new landscape is technology *terra incognito*. The United States is in danger. It is in danger of losing old capabilities and of not being able to acquire new offensive and defensive capabilities quickly enough, even where the technology was developed by the United States. More significantly, it is vulnerable to those new capabilities being acquired by more agile adversaries.

With commercial interest being the primary driver for technological advances, technology-derived capabilities are within the reach of all. The pace of technological advance now means that the cycle time of systems development in DoD is almost guaranteed to produce military systems that are three to four generations behind the state-of-the-art at the time of their introduction, even with recent improvements in the acquisition process. Moreover, the rate and range of technology dissemination makes it harder today to maintain a technological edge than it was in the past. Technology areas and capabilities previously at the periphery of DoD's focus, most notably biotechnology, are increasingly critical to future military operational capabilities. Most of the significant advances in biotechnology in the past five years have happened outside the traditional DoD-sector industries, outside DoD laboratories, and with little or no DoD S&T

funding or involvement. Finally, DoD's R&D management process – technology program area selection, initiation, review, reporting, and transition – is, for the most part, structured along individual technology areas. Useful technology is slow to transition to the military because the focus on military capability drifts to technological advance alone. DoD S&T management processes catalog rather than catalyze R&D activities.

In the coming decades the task force believes that there are four overarching technology areas that will generate new, unique, and overwhelming military capabilities: biotechnology; information technology; microsystems (electronics, photonics, MEMS); and energy and materials. Moreover, advances at the interfaces between these technology areas will be as significant, if not more so, than advances in only one area alone. DoD is presently ill prepared to either exploit or catalyze this revolution. In two of the technology areas – microsystems technologies (electronics, photonics and MEMS) and energy and materials – DoD will continue to be a major, if decreasingly important influence on the direction and pace of technological advance. In information technology however, DoD once led but is already dependent, and increasingly so, on the information infrastructure, services, and applications of the computer and telecommunications industry. And in biotechnology DoD does not have significant resident expertise or relationships with the biotechnology industry, nor is it on a path to do so.

DoD has an opportunity. It can harness and accelerate advances in commercial technologies, most notably in biotechnology and information technology, to insure that the offensive and defensive U.S. military capabilities continue to be unique and overwhelming. DoD, with its mission orientation, is unique in its ability to focus on capabilities and thereby influence the course of technological advance and drive the integration of technology areas. DoD will need to develop a strategic approach to R&D investments and make changes in their focus. It will also need to make changes in the S&T management process and in the relative balance and role of DoD versus industry interactions.

The task force believes a necessary organizing principle to realizing opportunities in the new technology landscape is the concept of Grand Challenge military capabilities. A Grand Challenge military capability should:

- Be militarily significant – the basis for enhancing or fundamentally changing military operations
- Provide a quantum jump in performance (at least 10-fold increase in performance)
- Be a driver for technological development and convergence
- Be challenging but feasible (no magic needed)
- Have a defined objective with measurable, intermediate stages of progress
- Likely be unmatchable by adversaries (either too costly or time consuming to do so)

DoD should focus a significant portion of S&T investments on five to seven Grand Challenge programs that anticipate and address projected limitations on future military capabilities. Selected properly, each of the Grand Challenge military capabilities should have cross-service roles and be of sufficient impact and challenge to warrant investments ranging from $200-1000 million per year. Each Grand Challenge program should last no more than 7-10 years. As such, the total investments envisioned are anywhere from $2-4 billion per year and would thus represent a major fraction of DoD's S&T budget. The different Grand Challenge military capabilities will likely have different balances of industry-DoD interaction, depending on the type and maturity of technologies to be integrated and whether they originate from either industry or DoD.

This report identifies and recommends focused technology investments in four Grand Challenge military capabilities. These are in ranked order of priority:

- **Bioshield**: real-time detection, characterization, response, and attribution of conventional and unconventional biological threats
- **No Place to Hide**: ubiquitous, intrusive, and inescapable on-site sensing
- **Fast Forward**: rapid, decisive force application from CONUS
- **Cognitive C^4**: warfighter-matched agile, secure and available C^4 systems

The task force does not believe that these four Grand Challenge military capabilities are the only ones that should be pursued by DoD, but it does believe these four capabilities are the four most critically needed and of universal utility to DoD.

BIOSHIELD

Bioshield is a potential technological development program that would provide for the comprehensive defense of U.S. military forces and the homeland against conventional and unconventional biological weapons (BW). The serious vulnerability of U.S. forces and the homeland to BW attack constitutes a strategic challenge equal to that created by nuclear weapons and ballistic missiles. The prospect of continued escalation in the potency, sophistication, and diversity of BW agents, and the unthinkable consequences of a massive attack, make an overwhelming case for elevating BW defense to a strategic priority that demands radical changes in national security policy.

This section calls for focusing a significant fraction of S&T funding on biological defense. It is a topic of continuing and growing national debate, as it should be. A major issue in that debate centers on assigning responsibility and the appropriate DoD role. In addition, the DSB currently has an on-going task force, jointly with the TRAC, on BW defense and is initiating a study of homeland defense, which incorporate the same issues. The views of the 1999 Summer Study task force on Defense Technology Strategy and Management are presented here as one input to the debate.

National Security Mission Needs

The following mission needs pertain to BW:

- Rapid detection and detailed characterization of deployed BW agents, to enable selection of prophylaxis, treatment, and containment actions
- Superior force protection equipment and low-cost, rapid decontamination methods compatible with sustaining protracted military operations in BW-contaminated environments, without compromising force capabilities
- New 'broad spectrum' drugs to inhibit highly diverse and constantly changing BW threats, including agents deliberately engineered to escape destruction by current drugs and vaccines
- Radical transformation of industrial production methods for drugs and vaccines to achieve on-demand, surge production within less than one week, ensuring sufficient quantities of prophylactic and therapeutic agents to respond to major incidents
- A homeland civil defense preparedness capacity, with a transparent command structure and emergency powers, logistics support, trained civilian personnel, and a proactive campaign to protect key infrastructure targets
- A large-scale microbial biosignature database and continuous global monitoring system for rapid detection of the production, transport, and release of conventional and unconventional BW agents

- A stronger global consensus and more international cooperation activities to impede and eliminate BW proliferation
- Legislation to establish responsibility for homeland defense and infrastructure protection and thoughtful definition of the DoD role, to allow proactive formation of robust civil defense preparedness

The Current Biothreat

Many national and subnational groups see biological weapons as their best chance to preclude direct engagement of U.S. forces and to offset U.S conventional superiority. Groups may attempt to exploit BW to undermine social order and economic stability rather than to attack military targets. The magnitude of the problem can be understood from the following illustrative scenario.

The task force laid out a scenario which is entirely possible today, using an attack against an overseas military base but equally applicable against a U.S. urban complex. As a result of this attack:

- In 48 hours, soldiers showing up in large numbers at sick call with flu-like illness. All were sent home with instructions for bed rest.
- At 72 hours, it was clear that this was not ordinary flu and antibiotics are issued without diagnosis. Supplies run out quickly.
- At 96 hours, first deaths occur and it is clear that antibiotics are not effective. The disease is identified. Hospitals are overwhelmed. Panic increases.

In the meantime, normal population mobility has spread the infection worldwide and the crisis goes rapidly out of control. There are no effective vaccines in sufficient quantity and millions die before the results are finally contained.

While the details of this scenario were developed by the task force, it was decided that they should not be published in unclassified documents. Suffice it to say that the sequence described, and illustrated in Figure 1, is not inconceivable today.

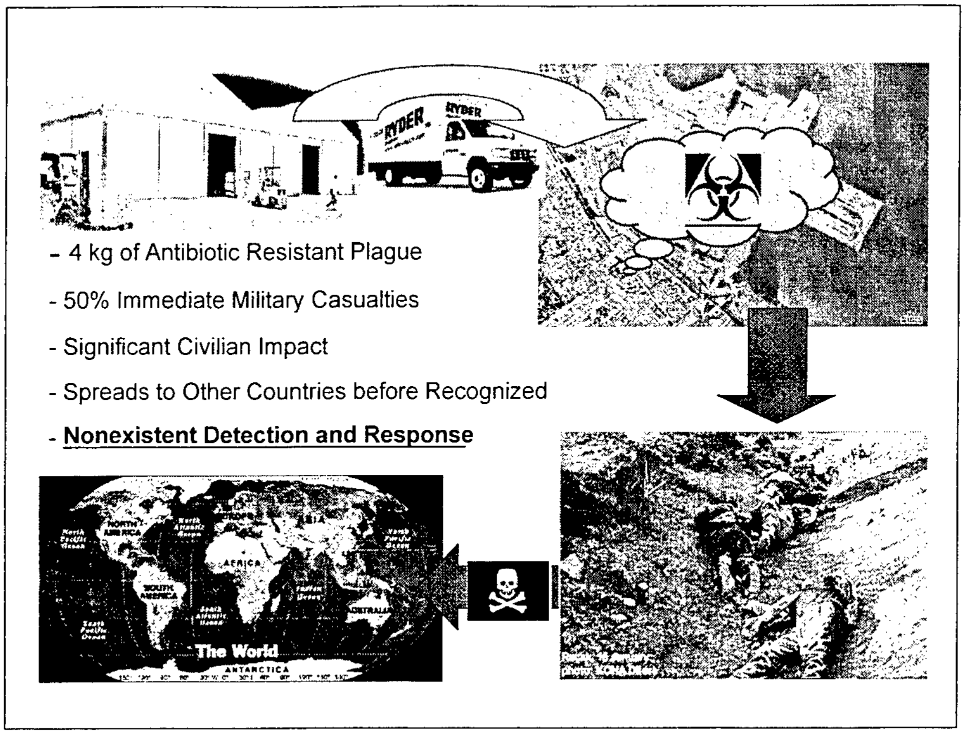

- 4 kg of Antibiotic Resistant Plague
- 50% Immediate Military Casualties
- Significant Civilian Impact
- Spreads to Other Countries before Recognized
- **<u>Nonexistent Detection and Response</u>**

Figure 1. Today's Bio-Threat Scenario

Unconventional Threats

The above scenario suggests that the United States is ill prepared to address existing conventional BW threats. Moreover, the potential for technological surprise is escalating, as genetic engineering, unconventional targets and mechanisms of action, and emerging diseases expand the spectrum and diversity of these threats.

The task force described in some detail the spectrum of possible advanced threats that the rapidly expanding biotechnology enables. Those future threat details aggravate an already serious set of deficiencies in U.S. preparedness.

The threat posed from emerging natural diseases may be as great as that from weaponized biological agents. Emerging diseases arise yearly somewhere around the world. Resistance to every known class of antibiotic has been reported and no new class of antibiotic since 1976 is in near-term development. Each new disease represents not only a natural threat to our security but also is itself a potential new weapon.

In the coming decades, economic and political instabilities provoked by major epidemics of natural infectious diseases will likely threaten national security and trigger the deployment of U.S. forces in a variety of operations other than war (OOTW). The marked increase in antibiotic-resistant infections, the breakdown of public health systems in third world urban settings, and the continued eco-shifts in which expanding human populations encounter rare or completely new pathogens will each enhance the probability of major epidemics and epizootics. Force protection, as well as the completion of policing and humanitarian goals, will depend heavily on effective protection against infectious diseases.

Current Gaps in BW Defenses

The Gulf War was a wake-up call to biological and chemical threats, underscoring inadequate U.S. defenses. Yet, nearly a decade and billions of dollars later, the United States remains highly vulnerable. Current generation detection capabilities are limited in scope and area. The principal modes of response are still voice alerts and donning protective gear, even though protective gear severely hampers troop movement and effectiveness. Current medical prevention and treatments will not save many of those exposed.

Gaps in Threat Surveillance, Detection, and Protection

Major deficiencies exist in current capabilities, spanning the spectrum from weapons production to deployment. These deficiencies include

- Inadequate human intelligence (HUMINT) and other global surveillance mechanisms to monitor potential BW production sites
- Increasing difficulty in distinguishing BW production activities from those of legitimate industrial biotechnology
- Poor or non-existant methods for detecting the transport and release of BW agents
- Inability to detect atypical and genetically engineered pathogens (unconventional BW)
- Insufficient stocks of drugs and vaccines to treat and protect exposed and at-risk populations
- Vaccine and drug production time cycles (months) that are incompatible with the need for on-demand "surge" production to respond rapidly to an incident
- Vulnerability of both military and homeland to unconventional agents engineered to circumvent current drugs/vaccines or evade the body's defenses
- High probability of uncontained spread from the ground zero attack zone for BW agents that have delayed incubation periods

Gaps in Threat Reduction and Elimination

- Erosion of international cooperation on export controls for dual-use technologies with BW relevance
- Lack of close-in sensors and forensic methods to enable covert detection of BW production and to enable reliable attribution to support interdiction and retribution on grounds credible to the international community

Gaps in Planning, Organization, and Technology Acquisition

- A large number of agencies and organizations devoted to BW making coordination difficult (despite some improvement)
- Poor engagement of the private sector in technology acquisition, research, development, test and evaluation (RDT&E), and product procurement
- Insufficient priority accorded to BW defense in current DoD and government budget allocations
- Lack of a comprehensive and integrated national S&T strategy and a transition plan to the user communities

BIOSHIELD: A GRAND CHALLENGE VISION

The escalating risk and serious vulnerability of the U.S. military and homeland to a BW attack, and the unthinkable consequences of a massive or multi-point BW attack, demand radical action. Fortunately the same rapid pace of biotechnology which fuels advances in the threat, also provides the opportunities for countering both today's threat and advanced threats if a concerted development effort is undertaken. The United States must mobilize the financial and technical resources to develop the necessary technology focused on a goal we have dubbed "Bioshield" – a strategic defense system against both conventional and unconventional bioweapons – and to deter the proliferation and use of such agents.

The BW problem is a multidimensional strategic challenge, with diverse threat scenarios that require very different responses. The dimensions of this challenge include:

- BW production – premption, detection, interdiction
- Battlefield attack – detection, protection
- Ground zero – treatment of exposed personnel
- Collateral in-theater forces – protection of unexposed personnel
- Homeland defense – detection, interdiction
- Homeland attack – detection, protection, containment
- Credible attribution – retribution

The United States must change its BW defense paradigm from reactive to proactive, from 'detect to protect' to 'detect to preempt.' Voice alerts should be replaced by automated neutralization responses; the use of immobilizing protective gear by unencumbered and effective fighting forces; and vulnerable buildings by shielded facilities. Post-symptomatic diagnosis must be replaced by presymptomatic diagnosis, limited treatment options by multiple broad-spectrum agents, and limited drug and vaccine stockpiles by an on-demand surge supply chain.

What has been sorely lacking is a strategic vision to grapple with the larger picture posed by the biothreat. DoD has traditional expertise in the identification of known, conventional pathogens and toxins and in vaccine development, but it has failed to give commanders a comprehensive solution. Commanders need the ability to detect threats in real-time, to neutralize or impede the threat of environmental contamination, to prophylax and treat casualties, and to attribute the source of traditional and genetically engineered conventional and unconventional biological threats. While this is a very difficult challenge, a great deal can be done today to ameliorate effects and well understood development paths exist for much more complete solutions.

What has changed within the last few years, and what makes a "Bioshield Project" urgent and possible, is the revolutionary knowledge gained from the Human Genome Project and biotechnology. The ability to understand diverse biological systems at the molecular level is now in sight. The DoD is simultaneously presented with a vastly greater threat challenge and the opportunity to comprehensively address the spectrum of BW threats. Moreover, success will demand quantal (discontinuous) shifts in capabilities, which will primarily come from the intersection of basic knowledge and technological development across four overarching areas of technology: biotechnology, information technology, materials sciences, and microsystems engineering. Progress will rely heavily on the evolution of novel technology platforms arising from the convergence of these four technologies.

The objective of the Bioshield Project is to develop the technology to prevent infection, transmission, and death. Specific elements of the project include:

- Wide coverage by affordable networks of detectors and sensors
- Biosignature recognition of engineered BW agents
- Automatic triggering of neutralization, protection, and containment responses
- Pre-positioned infrastructure protective systems
- Presymptomatic detection of infected individuals for infection control and early therapy
- Novel non-agent-specific immune enhancement pharmaceuticals, available to protect against novel agents and agents engineered for resistance
- Revolutionary production capability for rapid supply (less than 7 days) of synthetic designer vaccines/therapeutics
- Source attribution credible to the international community, through pathogen biosignature, intelligence, and forensics

Strategy for Development of a Comprehensive Solution

A well-conceived program of significant dimensions and national scope could produce the capabilities listed above and effectively solve the biothreat problem over the next 10-20 years. Key parameters for quantal shifts in technology performance for detection, characterization, and response are summarized in Table 4.

	State-of-the-Art	Trend	Needed
Detection (in environment)	Detect to treat	Detect to protect	Detect to preempt
	Big (HMMVEE)	Handheld, custom	Mini, solid state
	10s of minutes	Minutes	10 seconds
	$\$1\text{M/km}^2$	$\$100\text{K/km}^2$	$\$1\text{-}10\text{K/km}^2$
	Few (8) classical agents	All classical agents	All agents
	Intermittent, point	Continuous, point	Continuous, area
	High false alarm	Manageable false alarm	No false alarms
	No homeland defense	Limited homeland	Wide homeland use
Detection (in body)	Medical lab diagnostics	Molecular probe diagnostics	Lab-on-a-chip
	Culture	ELISA, PCR	Host defense biomarkers
	Conventional pathogens	Conventional pathogens	Conventional & unconv.
	Days	10 minutes-hours	1 min
	80% mortality	30% mortality	<5% mortality
Characterization	Classical Agents (~8)	All conventional agents	All agents
	Physical evidence	Physical evidence	Tracing to source
	No functional markers	Functional profiling 10-100 markers	Full function, 1,000s of markers
	Inadequate surveillance	Natural pathogens in friendly countries	Wide-area sampling, Constant updating
Response	Limited treatment	Few new vaccines & antibiotics	Designer vaccines
	Vaccines from <1960s		New broad-spectrum
	Antibiotic research stalled		Anti-microbials
	Inadequate stockpiles	Improved stockpiles	Surge mfg. capability
	Slow production cycle (months)	Reaction times little changed	Cycle times of days
	Domestic response slow (days)	Aware civil defense (hours)	Choreographed civil defense (minutes)

Table 4: Technology Evolution for Comprehensive BW Program

The following components are contemplated; these each will require substantive advances in technology performance.

1. Comparative and functional genomics. Define classes, families, and themes of biothreats such that a novel threat could be recognized as a variation on a theme. Identifying factors of microbial invasiveness and lethality is an anticipated outcome. This objective would relate not only to microbial agents but also to toxin production and resistance factors. A searchable microbial genomic database would be created, against which a novel threat agent could be compared. The tools for agent comparison would also be created. By implication, the genomes of multiple bioagents would be sequenced for comparison. To date, genomes from approximately 60 known, non-viral pathogens have been sequenced. For small microbial genomes, whole genome sequencing has become a relatively commonplace task. Militarily relevant organisms would be targeted, but some clinical pathogens should also be included to better understand the breadth of pathogenicity and to leverage off efforts outside DoD.
2. Proteomics/Structural Biology. Understand the mechanism of action of the factors of microbial invasiveness and lethality and visualize the three-dimensional structure of the sites of action. This component would deal less with the genetic information than with the protein product. This information could then be used to assist the biomedical

community and pharmaceutical industry to produce therapeutic regimes. In this way, synthetic bioactive agents might also be recognized.

3. Distributed Wide-area Sensor Systems. Produce a suite of dumb and smart sensors and detectors that can provide blanket coverage of an area by virtue of their small size and low cost. This capability would be developed to recognize specific agents and classes of agents and to provide information on viability, quantity, and genomic and proteomic profiles. Networking and communications would be elements of this program.
4. Synthetic Designer Vaccines/Therapeutics. Achieve vaccines or drugs that can be tailored to a specific bioagent and rapidly produced for use within seven days of a bioattack. The key to such rapid tailoring is to understand the limited repertoire of pathogenic mechanisms. Harnessing structural insights will also be of great value. To enable rapid production of vaccines or drugs, current bioproduction processes would be converted to chemical synthetic production processes.
5. Therapeutic Strategies for Body Defense Enhancement. Develop pharmaceuticals that will enhance the body's natural defenses when challenged by a threat agent. Immune and other body defenses respond to a variety of biological challenges in a limited number of ways. For instance, antibody production is the main defense against most bacteria and interferon production is the main defense against viral challenges. In fact, successful pathogens often employ mechanisms to evade normal host immune responses. This information could be used to develop body defense enhancement pharmaceuticals. Such drugs would be particularly important when the specific threat agent has not yet been identified or characterized, when the agent is antibiotic resistant, and when the specific vaccine/therapeutic is unavailable. They would also be important as an automatic response to the initial infection. It should be possible to detect a presymptomatic infection within the first hour by a cytokine profile. The profile may then be used to select a defense enhancement drug. Automatic dispensing from a skin patch is possible if an appropriate on-body sensor is coupled to it.
6. Presymptomatic Diagnostic Screening. Detect an infection within one hour – well before the onset of symptoms. This would be possible by screening for the production and detection of IgM antibodies, mast cell degranulation products, cytokines, nitrous oxide, or other mediators. The immune response profile could be used to classify the type of infecting agent. An on-body detector would be the distant goal of such a program.
7. Large Scale Microbial Biosignature Database. Increase knowledge of microbial threats and strains from regions of the world. Such knowledge would facilitate the recognition of a bioattack, the attribution of its source, and the scaling of pharmaceutical production. Project Alexander, the World Health Organization (WHO), and even the military have some global surveillance capability. However, more significant nonpublic surveillance is needed, including catalogs of strain fingerprints and genomic profiles. Tracking DNA sequencing equipment, polymerase reagents, and other items would be useful. Specifically, credible source attribution will require a combination of strain fingerprinting, intelligence, and forensic capabilities.

8. Broad Area Decontamination and Neutralization. Develop strategies and techniques specifically to counter bioagent releases over broad areas. To accomplish this, risk assessment and dispersion prediction need to become sophisticated, and strategies to decontaminate air, water, and ground releases need to be addressed. Projects to develop more efficient building filtration systems would be considered, as would innovative chemical decontamination strategies for complexes, bases, and cities. One possibility is the use of micrometer-wave gigawatt directed energy for the thermal sterilization of large clouds. The efficacy and practicability of such systems would require rigorous testing for a variety of agent types.
9. Instrumentation and Analytical Equipment. Reveal instrumentation and analytical equipment needs. For example, investments in genechip and advanced DNA sequencing instrumentation may be important.

INVESTMENT STRATEGY

DoD's present biodefense program costs approximately $1 billion per year, most of which is spent on vaccines, protective gear, and other defense related acquisition. The S&T (6.1-6.3) component of this funding is very small and has shown only a minimal increase in the last few years despite growing congressional and presidential concerns and recommendations by many groups, including previous DSB studies. The only bright spot is DARPA's investment, which now exceeds $100 million for all aspects of the work, including sensing and medical technologies. However, the scale of investment relative to the problem and its potential impact is totally disproportionate.

Therefore, this task force recommends the immediate doubling of the DoD biodefense program, to approximately $2 billion per year, with a strong emphasis on S&T and RDT&E. DoD needs to invest aggressively in advanced schemes and create an environment that supports promising projects and moves them quickly through the normally tedious 6.1-6.2-6.3 route. Significant risk-taking and failure must be tolerated and even encouraged if the program is to succeed. At the same time, the winners need immediate encouragement and support and should not have to wait until some agency submits for the next Program Objective Memorandum (POM) cycle. In other words, business as usual is insufficient and dangerous.

The task force recommends an additional investment of $6.9 billion over the Future Year Defense Plan (FYDP), continuing the development of aggressive advanced technologies for sensing, characterization and response. This figure is above any present biological budget and should not be considered a reservoir for existing program shortfalls. Despite the five-year recommendation, one should not anticipate the project concluding at that point. Budgeters and the Congress should at a minimum anticipate these very difficult objectives taking 10-20 years. However, one should also anticipate that once DoD has made the substantial initial investments, there would be a follow up from the private sector, as these technologies have enormous dual-use potential.

The task force recommends a five-year investment strategy as described in the following table.

Comparative and functional genomics	$0.6 billion
Proteomics and structural biology	1.0 billion
Distributed wide-area sensor systems	1.0 billion
Synthetic designer vaccines and therapeutics	0.8 billion
Therapeutic body defense enhancements	1.5 billion
Presymptomatic diagnostic screening	0.4 billion
Large-scale microbial biosignature database	0.8 billion
Broad-area decontamination and neutralization	0.4 billion
Instrumentation and analytical equipment	0.4 billion
Total	**$6.9 billion / five years**

Table 5: Bioshield Investment Strategy

The investment required to achieve these goals is substantial. The task force notes that one new drug costs the pharmaceutical industry from $400 million to $1.2 billion to get from basic S&T to market. New biotech startups get investment capital routinely, measured in hundreds of millions of dollars, and many of these never produce a single product. This is truly a very difficult field of endeavor, since when human lives are involved, the stakes are so great.

The Deutch Report published in July 1999 is highly critical of the lack of strategy, poor guidance, inadequate operational coordination, and flawed technology acquisition for BW defense. An extensive list of reforms in DoD and other departments and agencies was proposed to redress these deficiencies. Appropriate emphasis was accorded to the need for greater visibility, heightened funding priorities, increased awareness of end-user needs, and improved engagement of the private sector in shaping S&T and RDT&E, actions for improved battlefield and homeland BW defenses.

There is currently no comprehensive S&T strategy across the various programs involved in BW defense. The multiplicity of federal agencies involved makes the integration of BW defense policies and priorities difficult. The priority accorded to BW defense in current DoD and government budget allocations is insufficient. There is a lack of focus in technology acquisition, inadequate consultation with end users, and inefficient technology transfer. The engagement of the private sector in technology acquisition, RDT&E and product procurement is poor.

This project must be science and technology driven and measured against performance objectives. The scientific nature of the issue mandates a high level of expertise, but DoD does not have the intellectual infrastructure for biological threats in the same way it has for nuclear threats—and it should not attempt to replicate it in the biologic arena. This project must harness the expertise dominant outside the DoD, elsewhere in government, academia (medical schools, veterinary colleges, and universities), and private industry. Investments by the biotech industry in biomedical research, particularly by the pharmaceutical industry, now exceed that of the entire federal government. However, the pharmaceutical industry does not invest in vaccines and therapies for biologic agents of military concern because of economic barriers and intellectual property and public relations issues. By hiring civilians for specific projects of limited duration, DoD can tap into the private sector's talent pool and take advantage of the latest developments made there. Some elements of the project will eventually be taken over by industry for dual-use applications.

The program should be created outside the existing military biological organizations in order to prevent internal conflicts and maintain focus over time in favor of more traditional priorities within the existing organizations. Interagency Personnel Act (IPA) talent and strong S&T project management would be assured. A DARPA-like program should be created which has an aggressive S&T and industry-friendly culture.

Private Sector Partnership

The momentum of modern biological research, which is driving both threat expansion and counter-measures, will require DoD to engage more closely with the private sector for S&T, RDT&E, and novel product procurement. Unlike physics-based industry, biology-based companies have little or no historical link to DoD, other than as routine suppliers of conventional health products and services, which are also sold to others. The formidable size of unmet global health needs dictates that for the foreseeable future the pharmaceutical industry has little need to compete for DoD programs. Indeed, pursuing government contracts has little or no appeal to these companies because of the excessive bureaucracy, unacceptable intellectual property policies, and intrusive demands to examine corporate financial data. The task force cannot anticipate whether pharmaceutical and biotech industries will accomplish the goals of this program, though they may indeed contribute. Industry is, to put it bluntly, not interested in this problem. Reasons cited include the following: unwillingness to open books to Defense auditors, intellectual property concerns, small market size, lack of experience in pathogen research at high containment levels, and unfamiliarity with this set of pathogens.

Several key objectives for Bioshield, particularly in the development of drugs and vaccines, cannot be accomplished without significant private sector involvement. The S&T efforts that underpin Bioshield, together with varied RDT&E activities in DoD and other government departments, will require efficient, seamless technology transfer to the private sector for further refinement and large-scale manufacturing. **It is imperative that all government-associated organizations with these responsibilities understand fully the commercial and technical priorities of industry. Otherwise, the unacceptable deficiencies of the past will be repeated.**

"NO PLACE TO HIDE"

Surveillance and reconnaissance systems, both present and planned, are predominately based on active or passive electromagnetic remote sensing from airborne or spaceborne platforms. These systems have significant problems providing critical surveillance and targeting data, especially in real time. First, remote sensors perform inadequately in certain environments, such as urban canyons or under foliage. Second, enemies can engage in camouflage, concealment, and deception by timing activities to coincide with gaps in coverage or by masking or duplicating the remotely sensed signatures. Third, many types of information cannot be satisfactorily or cost-effectively obtained by remote sensing.

The technological developments required to mitigate some of these shortcomings is discussed at length in the work of the Information Superiority task force. An excellent solution is to complement standoff sensors by placing shorter-range sensors in the area of concern and to read out those sensors remotely, permitting continuos sensing of a wide range of signatures. Many interesting observables are present at close ranges, but are difficult or impossible to sense remotely. These include

- DC to mm-wave electromagnetic emissions
- Magnetic fields and magnetic anomaly detection
- Acoustic signatures, including Doppler shifts
- Chemical emissions: single substance detection to full chemical analysis
- Biological agents: detection, quantification, or comprehensive agent identification
- Nuclear radiation
- Pressure and vibration sensing
- Air flow sensing
- Short-wave ultraviolet emission
- Infrared emissions
- Imaging, object recognition, or image change detection

Though close-in point sensors exist today, their utility has been severely limited for several reasons. First and foremost, the power consumption requirements of the sensors, combined with limitations in battery technology, have resulted either in large, battery-dominated sensors (such as those used in Vietnam), or in smaller sensors with very limited functionality, transmission range, and mission lifetime. Limited range, "dumb" sensors are inconsistent with providing wide-area coverage. The size, cost, and performance of current sensors, combined with the difficulties in emplacing them, have limited their use to small numbers in proximity of high value targets. In addition, the technology has not existed for very low cost sensors or even for several observables, such as chemical or biological agents; emerging technologies promise to dramatically alter that situation. Finally, point sensors have been viewed as either stand-alone devices or for use in locally controlled clusters. An architecture to integrate these into a wide-area, information-on-demand surveillance system has not been developed.

A NEW WAY OF DOING BUSINESS: MASSIVE INFILTRATION WITH LOW-COST MINIATURIZED SENSORS

Advances in energy sources, microsystems technology, and biotechnology promise low-cost, miniaturized sensors that could be cost-effectively distributed over a theater of interest, providing real-time, continuous, all-weather, day-night surveillance. An enemy could not practically evade such coverage. Key attributes of the proposed capability are:

- Ability to measure a *wide range of signatures* making concealment and deception a very difficult problem for an enemy and greatly reducing his mobility and agility.
- *Continuous* real-time monitoring, with information provided *on demand* through a wide-area network controlled from overhead or terrestrially. Utilizing an aircraft, or a space-based system employing a large aperture sparse antenna array, the sensors can be geolocated and "polled" to deliver their unique identification and stored data. Alternatively, ground-based networking options allow a secure, low-power communications network with a robust connectivity, and low probability of detection (LPD). This network could be used by forces operating in the area. Because data delivery would typically be in short bursts and the timing of transmissions would be remotely controlled by the user, major power reductions and improvements in covertness could be expected compared with present systems. Sensors could be kept dormant until needed or commanded to report back only if high-value events were detected.
- *Small size and low-cost* sensors (on the order of one cubic inch and costing less than $10 each). Such sensors could be dispensed in overwhelmingly <u>large numbers</u> (such as 100,000 sensors over a theater of operations) which would not only enable <u>wide-area coverage</u> from what is essentially a point sensor, but also make location and neutralization very difficult for the enemy. Even less expensive decoys could further complicate detection and cleanup by an enemy.
- *Covertness*. This would be achieved through small size, camouflage, mobility, and LPD communication enabled by on-board intelligence. However, depending on the application, the very use of large numbers of sensors, coupled with extensive intermixing of "penny" decoys, might obviate the need for covertness by simply overwhelming the enemy with too many sensors to pick up or destroy. A sensor survival rate of as little as 20-30 percent could still provide the required functionality.
- *Survivable*, and <u>capable of long duration operations</u>. Depending on the sensor type and intended application, and particularly on advances made in power supply technology, conceivable operational periods of the network (not necessarily of an individual sensor) range from months to years.

- *Deployment and emplacement.* Non-traditional deployment means may be used – such as "crop dusting" or "air burst," inadvertent transport into inaccessible areas by the enemy (sensors clinging to vehicles or clothing), or the sensor's own robotic or biologically aided mobility. Other means could be used as well, such as artillery delivery and hand emplacement (sowing), either overtly by troop units or covertly by operatives behind the lines.

Such a system could have covered Kosovo with sensors spaced approximately every 30 meters, at a total cost for the sensors of only several tens of millions of dollars. The data from these sensors, integrated into a C^{4}ISR system with other data acquired from more traditional stand off sensors, would have provided a comprehensive view of the battlefield, enemy capabilities, and enemy intentions. Of particular interest is that such a sensor system would have the capability of gathering information on weapons of mass destruction, of characterizing concealed and hardened facilities, and of providing information on targets obscured by foliage.

Roadmap of Required Technology Developments

Achieving sensor system goals will require significant developments in the overarching technology areas of energy, microsystems, and biotechnology.

	Today	**Current Technology Trend**	**Needed Advances**	**Key Technology Area**
Networked	2-10	100s	10-10,000x increase in number	Information tech. Microsystems
Lifespan	Hrs – days	Low-power electronics + energy extraction => 2 weeks	10-100x increase	Microsystems materials & materials
Ensemble	4-5 physical sensors	Polymer films for chem sensing, bio assays-on-chip	10-20 bypes of sensors: physical, chem, bio	Biotechnology, materials, & energy and microsystems
Undetectable	Coke-can-shoe box size: fixed	>1mm^3 seismic sensor, 3D packaging	10x decrease in size intrusive e.g. biosentinels	Microsystems, materials & energy biotechnology
Affordable	$1,000/sensor	~$5 MEMS accelerometers	100x decrease	Microsystems
Deployment	Hand-emplaced	Lighter, smaller => min shock resistant, aerodynamic structures	UXV emplace, high alt. Air dropped, 100-1000x increase (in emplace rate)	Materials & energy microsystems information technology

Table 6: Technological Developments Needed for Close-in Sensors

Table 6 captures the principal attributes required for a sensor network and shows that changes of 10-to-100-fold are needed in several of the technologies to make ubiquitous, inescapable, intrusive sensing possible. Some key areas where research is needed are energy sources, microsystems, and biotechnology.

Energy sources. A mix of sensors is envisioned, ranging from low data rate seismic sensors to high data rate video sensors. While some of these sensors would achieve the desired lifetime with today's batteries, others will need about 10-100 times more energy than can be provided by present day batteries. Two approaches have been identified that could lead to such an improvement: very high-energy-density materials and energy harvesting from sources (physical and chemical) in the local environment.

Microsystems. Achieving the critical size, weight, and cost targets that are necessary for close-in sensors will only be possible if nano-scale miniaturization and mass production techniques are developed. Developments in Micro-electro-mechanical systems (MEMS) for sensors, especially for the microfluidic manipulations needed for chemical and biological identification, will be critical. A special focus on increasing the level of integration while controlling process cost is critical to success. MEMS will also play a critical role in interfacing with biological systems, providing mobility, and reducing the cost and complexity of the communications subsystems. Lower power and more highly integrated electronics, as well as efficient algorithms, is essential to enable the sensors to locally process signature data, thereby minimizing the quantity and frequency of data transmission. This would reduce both power consumption (communication is very costly) and probability of detection during communication. For certain sensors, a reduction in power-per-operation of more than 10,000-fold may be needed from present day levels.

Biotechnology. Developing low-cost sensors capable of detecting and fully characterizing bioagents will become possible with sustained and focused work in the biotechnology area. Biotechnology may also provide other quantum leap technologies that could provide dramatic new capabilities in miniature form factors. For example, the successful integration of electronic microsystems with living organisms, such as insects, could provide new delivery systems for the sensors, or impart mobility. Biological systems or processes could provide the basis for generating energy at the sensors by using materials present in the local environment, just as living organisms do. Chemical sensors (odor detectors) are yet another example of sensing capabilities that might become possible through biomimetics.

INVESTMENT STRATEGY

Many technologies needed for these miniaturized sensors are already under development with support by DoD or the commercial sector. For example, a current five-year program in the Army is developing an increasingly capable network of small sensors that can detect many, but not all, of the signatures described above. These sensors are small, easily deployable, able to function unattended for three to four months, and are locally netted together on the battlefield. To achieve more sophisticated sensor capabilities (such as video-based and bio-sensing capabilities), longer lifetimes, and truly strategic capabilities such as country-wide coverage by sensors with real-time, remote polling, and on-board data processing – these developments will need to be continued and expanded. This will lead to evolutionary improvements in conventional point sensors, as well as lay a technological base for more radical concepts. However, to achieve the dramatic technological capability needed to make feasible the ultra low-cost, highly capable, and widely proliferable sensors described above, focused investment is necessary in "stretch" or "radical" technologies. Focused investments on approaches that could lead to leaps in capabilities in energy systems, microsystems, and biotechnology are essential. A joint Service ground-based sensor program should be established, responsible for funding development activities in energy sources, microsystems, and biotechnology and for integrating these into a pervasive sensing system. Appropriate levels of funding are on the order of $100 million per year for each of these three technology areas, sustained over at least a five-year period. It is worth noting that these technological developments are expected to have a broad impact across a wide range of DoD systems and to enable significant civilian dual-use payoffs.

FAST FORWARD

NEEDED CAPABILITY

Regional operations requiring rapid global force projection are shaped by a variety of missions and entry conditions – all of which can change as regional situations develop. Figure 2 below indicates some of the factors that can influence regional operations.

Missions	**Theater Environments**	**Proximate Infrastructure**
Warfighting	Opposed	Non-existent
Peacekeeping	Disrupted	Austere
Humanitarian	Benign	Robust

Figure 2: Context for Regional Operations

To effectively respond to these regional contingencies, forces will need to be fast and effective, yet humane. Table 7 describes the desirable attributes of these forces.

Fast

Rapid planning
Rapid arrival and assured entry
Intra-theater agility
Small forward footprint

Effective

Pervasive, intrusive surveillance and intelligence
Adequately sized, tailored and trained force
Appropriate presence and force application
Timely, efficient sustainment

Humane

Minimal casualties for coalition, neutral, and sometimes, enemy personnel
Low collateral damage

Table 7: Desirable Characteristics of Regional Operations

The need for rapid deployment and sustainment of increasingly capable forces is well documented in the body of the Summer Study report and generally widely accepted. The recommendations there provide for redesign of the forces and incorporation of the latest technologies. These are transformations that can take place in the next decade. Numerous technology and systems development programs in the government and private sector are contributing to these future capabilities. These programs include continuing advances in computing, automatic target recognition, hypersonic flight, automatic information processing and displays, sensors and platforms, communications, realistic and integrated training systems, and directed energy weapons. In addition, developing the other Grand Challenge technologies recommended in this report will result in major contributions. However, there are technologies on the horizon which offer potential for very significant improvements beyond that achievable in the nearer term.

Major advances in materials, energy systems, and robotics will be central to enabling substantial further improvements in deployment and sustainment of U.S. fighting forces by air. Specifically, increases in the strength-to-weight ratio of materials and in the energy density of fuels, propellants, and explosives, along with the miniaturization of power sources, will drastically lighten the entire deployment package. This will extend the range of U.S. ground and air vehicles and weapons, make space weapons practical, extend the operating life of equipment, and increase the potency of warheads. While advances in each of these technologies have been very modest for decades, new materials and design approaches and new fuel formulations hold promise for order-of-magnitude improvements over the next two decades as shown in Figure 3.

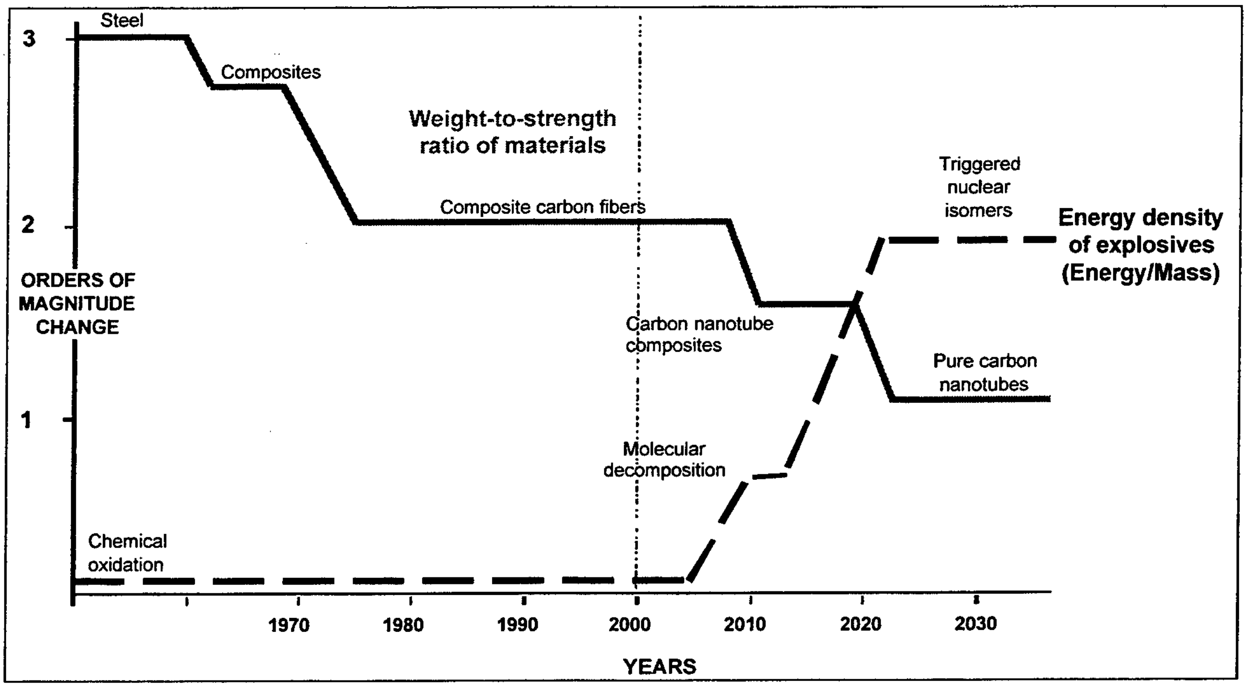


Figure 3: Potential Gains in Performance of Structural & Energetic Materials

Technologies

While many technologies will contribute to enabling future capabilities, the task force has identified three in particular that have the greatest leverage and can provide completely revolutionary capabilities for the military. These technology areas are structural materials, energy, and robotics. They promise to reduce the weight and cost and increase the effectiveness of essentially all military vehicles and craft by an order of magnitude when applied together. Even greater gains are possible in selected applications. These technologies are discussed below.

Structural Materials

Carbon nanotubes, also known as Buckytubes, single-handedly promise immense weight reduction. Their existence was discovered only nine years ago, and their properties are already proving phenomenal. They have 100 times the strength-to-weight ratio of steel, and about 25 times that of graphite-epoxy carbon composites. In addition, they stretch up to 30 percent before breaking and buckle without permanent deformation. The nanotubes are the stiffest and strongest known material. The characteristics of nanotube structures are included in Table 8 below.

Technology	Today	Promise	When	Funds	%DoD
Strength of structural materials*					
Steel	0.15-0.3 M psi	--	Now	--	--
Graphite composite fibers	0.5-1.0 M psi	--	Now	--	--
Carbon nanotube composite fibers	--	2-10 M psi	5 years	$20-50 M/yr	90
Pure carbon nanotubes	--	25 M psi	10 years	$20-50 M/yr	90

* Working tensile strength

Table 8: Potential Advances in Super-Strength Materials

Nanotubes are minuscule, about 1 nanometer in diameter and 1 micron long at present. They can be made in the laboratory in small quantities, but very slowly. The growth of pure carbon nanotube materials for structures is still in the early research phase. Attempts at forming nanotube composites are starting in order to capture at least a portion of their benefits.

The projected capability of nanotube structures, if their funding is greatly increased and focused (discussed below), is illustrated in Figure 3. One order of magnitude weight reduction for strength-dependent use is foreseeable, compared with current graphite composite materials. It is likely that a concomitant cost decrease will occur when nanotubes are better understood, and once techniques for their utilization emerge.

Carbon nanotubes are in early research phase, and despite their very large promise, funding for research into their structural applications is almost nonexistent. Although some $10 million per year is being spent on nanotube research in the United States, most of it is applied to electronic and other non-structural characteristics and uses of nanotubes. Only about $500,000 is applied to research into structural aspects of carbon nanotubes. In contrast, Japan and Europe equivalent programs reportedly exist at the $100 million per year level. These levels represent national commitments and are indicative of the enormous leverage that such structures will have.

A focused U.S. national initiative is warranted, led by DoD, in order to ensure that the United States reaps the benefits of such super-strong materials. Moreover, without such an initiative, the United States may find itself at a large strategic and tactical disadvantage should other nations possess such structures a decade hence and it does not. The research must entail a number of parallel approaches to grow the oriented pure nanotubes so that they form long strings, sheets, rods, and patterned-formed structures, each with the full stiffness and strength of the pure nanotubes. The growth techniques must be chosen such that they are amenable to volume production at low cost. Once the techniques are thus demonstrated, leadership must be transitioned to industry for application to a variety of products.

Carbon nanotubes will be able to be made into trucks, cars, tanks, aircraft, spacecraft, launch vehicles, rifles, artillery, missiles, antennae, wheels, engines, suspension parts, electronics, pressure vessels, and indeed most articles now made from metal. As a result, the weight of strength-related components in these articles would be reduced to as little as one-tenth of today's embodiments. This would indeed be revolutionary. For example, applique armor might be cut to one-fifth its current weight. A spacecraft bus weighing 10,000 pounds today might weigh 100 pounds. Launch vehicles could be easily built that cost less than $100 per-pound-of-payload to orbit. Tactical aircraft empty weights could be reduced by half. Many other examples can be envisioned to illustrate the dramatic effects of carbon nanotube technology.

Such structures alone, without any advances in energetics or changes in force composition, have the potential to cut the weight of the logistics tail of engagements by at least a factor of two and much more when combined with the high-energy-density materials discussed below.

Energy

A number of possibilities exist for increasing the energy density of fuels, propellants, and explosives, as well as that of micro-sized energy sources for miniaturized remote sensors, as shown in Table 9.

Technology	Today	Promise	When	Funds	%DoD
Energy density of materials					
Fuels	43.3 kJ/g ($JP-8$/air)	120 kJ/g (H_2/air)	5 years	\$3-10 M/yr	20
Propellants	290-460 sec (Solids-H_2/O_2)	500-1,000 sec (meta N_2-H_2)	5 years	\$2-4 M/yr	100
Explosives	5-6 kJ/g (TNT-HMX)	20-94 kJ/g (Meta N_2-H_2)	5 years	\$2-4 M/yr	100
		500 kJ/g (Triggered Isomer)	10 years	\$2-10 M/yr	100
Micropower sources	660 Wh/kg (Lithium Primary)	3,300 Wh/kg (H_2/air)	5 years	\$5-10 M/yr	50

Table 9: Potential Advances in High Energy Density Fuels (To technology readiness)

Molecular decomposition techniques have been recognized for years as the first step in attaining greater energy density than traditional high explosives – promising anywhere from a four-fold to a 20-fold increase. Metastable solid states of nitrogen are known to liberate four times more energy upon reversion to the gaseous state than does TNT. A step up is the exploitation of metastable solid hydrogen, which would offer 19-fold more energy upon decomposition to the gaseous state than does TNT.

The ultimate in intermediate-scale energy sources are the so-called triggered nuclear isomers, in which large quantities of low energy gammas are released upon a triggered relaxation of the spin or shape states of the nucleus. These nuclear isomer techniques liberate more than 100 times the energy per weight than chemical combustion, yet stop short of the nuclear radiation residuals and other major consequences of nuclear explosives.

Another important area of high-energy-density materials is that of micro-power sources for long-life remote miniature sensors and other demanding small-scale applications. These power sources include miniaturized fuel cells, nanomachined turboalternators, and other technologies. Though there is some university activity in this area, a more focused and better-funded activity is needed. This activity should be aimed at micro-power sources the size of a watch battery but with at least five times the energy storage capacity of the best lithium primary batteries.

Robotics

Rapid deployment of overwhelming combat forces can also be greatly enhanced through the use of robotic vehicles for three purposes

- Carrying both broad area and local area sensor systems into combat areas before enemy air defenses have been defeated
- Flying low-cost precision weapons into position over enemy formations also before enemy air defenses are defeated
- Supplying ground forces after their injection into combat areas

In all these applications, potential losses of manned air vehicles during initial combat can be avoided. Such robot vehicles can be made smaller and lighter by eliminating human pilots.

Crosscuts with technologies of other missions

Materials and energy interact with the other three areas of technology examined by this task force. An example is the development of tiny and proliferated remote sensors for the intrusive, close-in surveillance described in "No Place to Hide." The ability to make sensors very small, and therefore inexpensive and survivable, is completely dependent on watch-battery-size energy sources that will power them for months or years. The existence of such sources will also allow much more processing power on the sensor, as well as the use of greater bandwidth and more power hungry techniques, such as motion video.

These capabilities are even more desirable for the "Bioshield" concept, which contemplates fielding sensors that could be carried by or implanted in small insects, or even shrunk to ameba or microbe size. Clearly the challenges multiply with such size reduction.

Materials and energy technologies intersect with each of the other three technology areas in which rapid progress is evident today and which will enable revolutionary capabilities in the near future.

Relevance to Needs and Vision

The ability to attain at least an order-of-magnitude reduction in the mass of weapons and logistics, as well as to increase the ranges of vehicles and aircraft, will alone significantly reduce the deployment and sustainment needs for rapid (~1 day) deployment of substantial military forces.

INVESTMENT STRATEGY

Rationale

The principal strategy that shapes the technology development and investment planning grows out of recognition that the three highest leverage technologies – super-strong materials, high-energy density materials, and robotics – are pacing items. While these are unquestionably breakthrough materials yielding order-of-magnitude weight reduction and effectiveness increases, they are in their very early research phases at present, and are also minimally funded. Several years will likely be required before even highly focused and well-funded efforts yield breakthrough materials that are ready for military application. In addition, there is a sense of urgency since other nations are reportedly pouring major funds into these areas, and the United States could be at a large disadvantage in tactical conflicts if other powers reaped the benefits of these technologies and the United States did not.

Given all of these factors, the United States should pursue an aggressive investment strategy for these technologies. This strategy has four elements described in Table 10 below.

Greatly accelerate research	The national importance of these breakthrough materials must be recognized and the research and technology activities must be accelerated as much as possible. This should ensure that progress in these areas will be limited by brainpower not money.
Demonstrate the technology soon	The technologies must be demonstrated (with intermediate outputs) in a relevant environment to verify that they indeed result in the predicted order-of-magnitude weight reductions and effectiveness increases. These weapon-application demonstrations can begin to ramp up as the materials characteristics are being defined in the laboratory, anticipating their likely manufacturability and other practical characteristics. However, there are some weapon technologies, such as electromagnetic weapons, that might proceed into definition and test in parallel with the materials technologies, as they can be, to some degree, independent.
Provide major DoD funding	There is little likelihood that the commercial sector will fund and pursue some technology areas, at least not until they reach the stage where economic benefits are clearly demonstrated.Therefore, these areas must be supported and funded largely by DoD. An example is the increase of explosives yield without concomitant weight increase; most explosives technologies are driven principally by military needs, with commercial sector uses following.
Piggyback on commercial activities	DoD activities must piggyback on commercial technology developments as much as possible, in those areas where commercial funding is likely.

Table 10: Investment Strategy for Energy and Materials

The application of this four-part investment strategy results in a technology development plan and roadmap, discussed below.

Development Plan

A plan for technology development, and an associated technology products roadmap, is shown in Figure 4. This plan represents a national-level commitment activity and treats only the super-strong materials and high-energy-density materials activities. Activities in robotics and information, which would support more efficient engagements and sustainment, are recognized as important but are treated elsewhere.

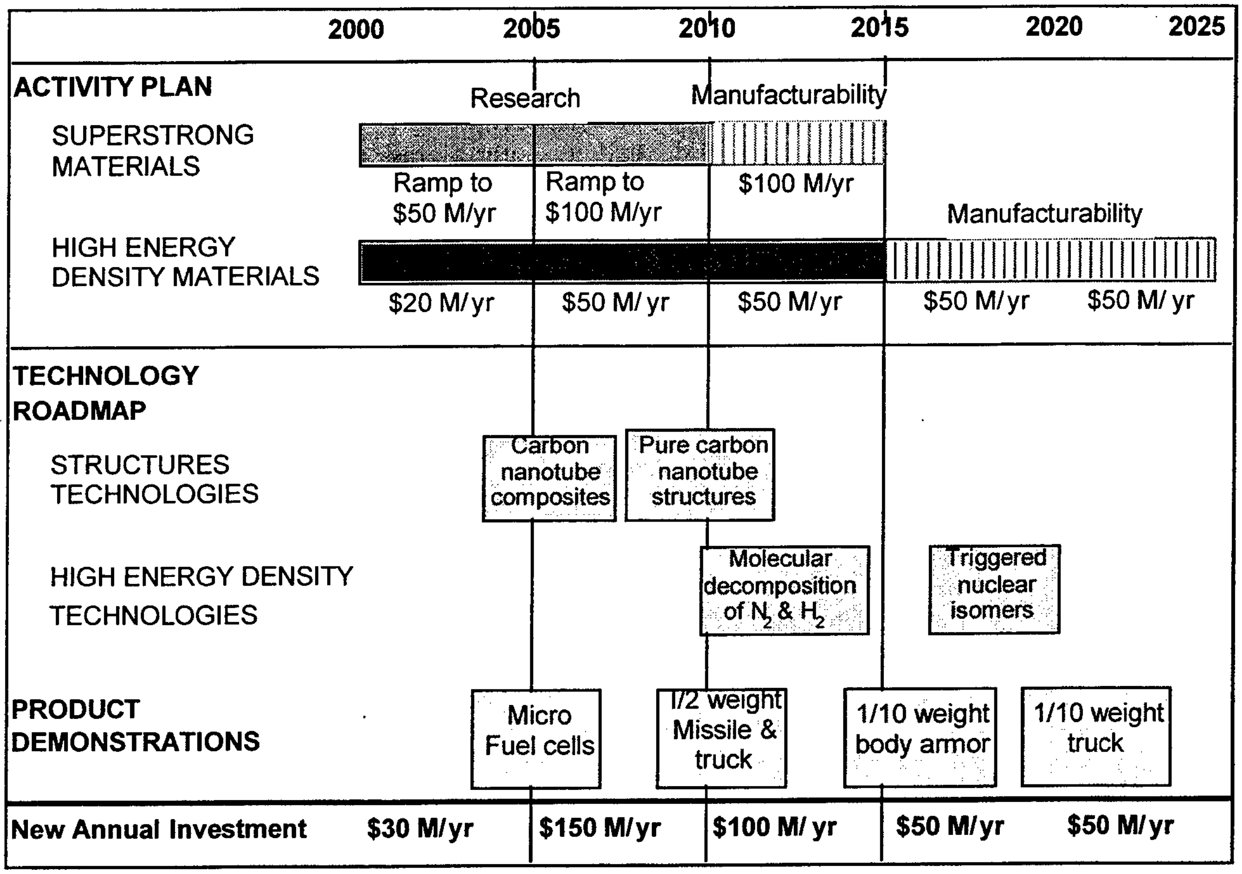


Figure 4: Technology Development Plan and Roadmap
(Funds required are additional to current)

The rough order-of-magnitude funds required are annual expenditures. They generally ramp up with time, as the technologies shift from 6.1-like research phases to applied research and move into technology demonstration phases. None of these funds includes the demonstration of entire capabilities, for which ACTDs or similar programs would need separate funding.

Early phase materials and energy activities may be limited more by brainpower than by funds, at least for the first few years. However, the payoff is so great that a special national-level initiative should be created immediately that focuses on the pursuit of these technologies and provided with the funds shown in Figure 4. These programs and their funding are further discussed below.

Super-strong materials

Total U.S. funding for super-strong materials, from government and matching university funds, is less than about $500,000, even though total nanotube funding is on the order of $10 millon. This is because the bulk of the research is focused on electronics and computing applications. While the structures applications are recognized as having huge leverage, they are being dwarfed by computer-centric initiatives where near-term, commercial payoffs can be anticipated.

The estimates in Table 11 represent a national-level initiative. They were derived from discussions with the Army Research Lab (unofficially), University of North Carolina Nanoscale Research Center personnel, and Rick Smalley and his team at Rice University. There are a number of different basic physics approaches to growing the oriented nanotube structures to order. They should be pursued in parallel by several university teams, with deliberate overlap. Funding should be adequate to attract the best chemists and physicists, sufficient numbers of graduate students and professors and to provide specialized laboratory equipment.

It is estimated that the first five years of this phase would require funding ramping up to $50 million per year, spread over at least five universities in parallel. Once the most promising techniques have been successfully proven, two intensely competing laboratories would be selected to focus on techniques to make the nanotube materials in quantity and in many different forms. This second five-year phase would have heavy industry participation and require additional funds ramping to $50 million per year, so that the total investment would peak at about $100 million per year. At that time, the techniques could be applied in the development and then production of structures for military applications. This phase would begin in the 2010 time period, and would be led by industry.

Outputs and products →	Sustained growth-random tubes	Prototype macroscopic strindab	Lbs/day random tubes produced	Large articles ¢g.body armor) made with strength X2 current composites		Smart materials produced	Tons/day production of random tubes	Demo of oriented membrane growth	Demo growth of oriented I-beams		Large complex objects (e.g.auto panels) grown with oriented tubes		Full scale oriented growth membrane plants in industry			Production → begins
YEAR FROM START	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
•Theoretical research on single-wall nanotubes	1	3	3	3	4	4	4	3	1							
•Production research																
-Random tube tangles	1	5	10	20	30	10	5									
- Oriented growth	1	8	20	30	30	30	30	20	10	5						
•Structural materials																
- Composite materials and techniques	1	5	8	15	15	10	5	2								
- Spinning fiber formation	1	2	3	3	3	2										
- Fabrication of pure-tube composites	1	2	5	8	10	10	10	5	2							
- Materials with tailored properties	1	1	1	2	2	2	5	5	5	5	2	1				
- Evaluation of weaknesses in materials	1	1	1	1	1	2	2	3	3	3	3	3	1			
•Development of specific materials and structures																
- Fiber materials (competing laboratories)				5	10	20	25	30	20	20	20	20	20	20	10	
- Structural materials (competing laboratories)						10	30	50	50	50	50	50	50	50	30	
•Oversight and coordination	1	3	5	6	6	6	6	6	4	3	3	2	1	1	1	
TOTAL FUNDS REQUIRED, $ Millions	**9**	**30**	**56**	**93**	**111**	**106**	**122**	**124**	**95**	**86**	**78**	**76**	**72**	**71**	**41**	

Table 11: National Buckytube Structures Initiative ($millions)

Because of its revolutionary potential for both strategic and tactical U.S. capabilities, the task force has defined a DoD-led national-level initiative which addresses the necessary buckytube (carbon nanotubes) structural research and experimental development, the funds required, and the specific products and outputs expected from such investments. This initiative, shown in Table 11 above was assembled from information developed with help from expert researchers in this field. It identifies major interim products that would be available along the way to developing the ultimate materials, each of which is a major advance over current capabilities. It also anticipates that following an intensive 10-to-15 year research and development effort, industry would support the bulk of the remaining tasks as a part of major DoD and commercial procurement activities.

The funding levels for these initiatives are miniscule when compared with other DoD S&T expenditures – especially considering their revolutionary potential. They should be pursued with utmost dispatch.

High-energy-density materials

The activities in this area parallel those in the carbon nanotube structures area in that they have enormous leverage in reduced weight and size, greatly increased vehicle range, or both. The technology and roadmap activities are also shown in Figure 4. These activities are composed of different lines for fuels, propellants, explosives, and micro-power sources.

Program emphasis should be aimed at relatively easier achievements, such as molecular decomposition of nitrogen or solid hydrogen. This would be followed by the much more difficult triggered nuclear isomers.

The funding levels are estimates based on discussions with laboratory personnel and are admittedly crude. The problems are as tough if not tougher to solve than in the structural materials area and thus greater funds are probably necessary. The funds are aggregates of the four energy areas discussed above.

It must be mentioned that while the U.S. laboratories have known theses techniques for many years, little progress has been made in bringing them significantly closer to reality. This is because there has not been a lab focus to make this happen and there has been minuscule funding. Total U.S. funding in this area is estimated to be less than $300,000. The $20-$50 million suggested in the figure is more indicative of the level that is needed in order to make serious progress in this area.

Intermediate products

It is expected that while the ultimate pure carbon nanotube structures are at least a decade away, even with such an aggressive plan, intermediate products such as nanotube composites would be available much earlier. These composites would be revolutionary in themselves, showing an improvement over current composites at least as large as that which current composites have over aluminum and steel structures.

A series of product examples with different time frames illustrates the potential benefits of utilizing super-strong materials and high-energy-density fuels and explosives. The first product could, for example, be a developmental micro-power source for sensors of the type envisioned for the "No Place to Hide" concept. This could be a self-contained sensor in a cubic inch package, with a life of over one-year at power levels five times greater than current batteries can support.

A second product might be a missile, such as an air-to-air missile, whose weight is cut in half without sacrifice in accuracy, range, or lethality. This would be achieved by using a high-energy-density propellant, high-energy-density warhead, and nanotube materials, which would lower structural and case weight. A truck with an empty weight fraction of 0.35 versus the current 0.7 would provide a similar factor-of-two demonstration.

A third product could well be a body armor that weighs one-tenth of conventional armor with the same effectiveness. Conversely, the armor could have 10 times the protective effectiveness but the same weight.

A fourth product could be a truck or other vehicle that has the same weight and volume as a current truck, but weighs one-tenth of the empty weight. This could also be applied to an aircraft, but the program would be considerably more expensive and difficult, though it may be more meaningful and dramatic. While practical considerations such as materials cost or manufacturing complexity may limit these weight reductions, any of these improvements would be revolutionary in their tactical and logistical implications even if they fell far short of these goals.

This or a similar sequence of demonstrations will probably be needed to prove the worth of the new materials and energetics to DoD and to initiate the commercialization that will lead to affordability for wide proliferation. The funding for these activities is additional to the research and lab-level experimentation covered in the development plan funds in Figure 4.

COGNITIVE C^4

VISION

Many necessary DoD capabilities have analogues in the evolving commercial and consumer worlds. These include the need for situational awareness from the commander down to the individual soldier; the need for mobility of forces; and the need to augment human capabilities to provide near-real-time decision-making. The paragraphs below describe some of the general trends that will evolve over the next 20 years that can have a transforming effect on military operations. The roadmap section describes the Grand Challenge technical goals. In summary they are:

- "Human-speed" computers: personal computers that provide 10,000 times the performance, using less than 50 watts of power
- Mobile, human-rate communications: megabit-per-second, universal availability
- Assured navigation capability: robust Global Positioning System (GPS) and inertial systems
- Augmented human capabilities: near image-analyst quality automatic target recognition (ATR), information search, and decision-support systems
- Universal connectivity: complete interoperability in military information systems with commercial and consumer information systems
- Human-matched interfaces: ubiquitous computer environments with presentation technologies matched to human capabilities
- Trusted environments: multi-level security systems that employ biometric user identification systems, water-marked documents, and embedded computer and network security tags

Supporting Technology

The requirements listed above outline some of the technology needs for a cognitive C^4 system that collects and distributes the appropriate information to users in near real time. Such a system will also need to intelligently adapt information so that it extends and augments human capability to use it. Over the next 20 years, a profound change is going to occur in the processing and display of information that is meaningful to humans. Because of this transformation, the task force has termed this program "Cognitive C^4." The following sections describe a number of Grand Challenge technical problems that should be addressed over the next 10-20 years. To set the framework for the task force's recommendations, the following paragraphs describe basic concepts and capabilities under development today.

Human-Equivalent Computer Environments

The web-centric concepts described above will create the basic infrastructure for wide-band, person-to-person communications, plus the opportunity for each individual to be their own broadcast network. But advances in computing are going to allow these advances to have even greater impact. They will open up unprecedented means of interacting with humans, not only at the data level, but increasingly at the information and knowledge level. Figure 5 illustrates this point.

Figure 5 is a plot of Moore's Law for computing. It indicates a rough doubling of computer price-performance every 18 months. One important consequence of this chart is shown on the right-hand ordinate. This axis shows the cost of building a "human-equivalent" computer. What does that mean? The human brain runs at about 10^{13} to10^{14} bits per second. This chart says that by approximately 2015 it will be possible to have a personal computer on one's desktop that costs less than $10,000 and that will go as fast as the human brain. Clearly, until computers can go at least that fast, they cannot perform certain human cognitive capabilities. After that, each additional 18-month time interval results in a computer that goes another two times faster than the human brain (assuming no electronic or genetic modification of humans). This discussion, of course, relates to pure "computing power" and does not recognize that the human brain has additionally evolved wonderful processes (algorithms).

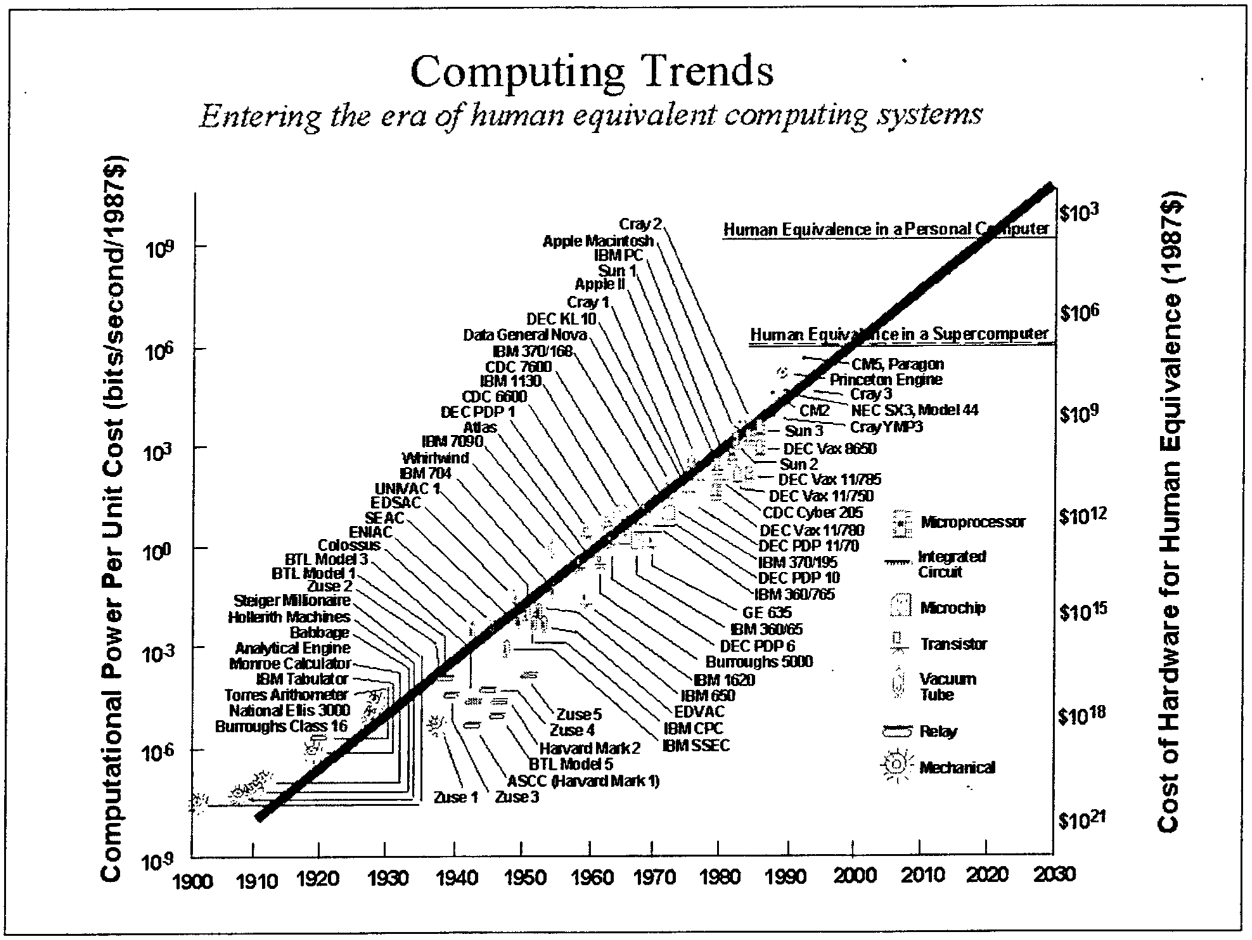


Figure 5: Computing Trends

The combination of wide-band web-centric communications, wall-sized immerse displays, sensory interface technologies, and enormous computer power will allow the development of applications that will profoundly affect methods of work and the conduct of warfare. For example, worldwide collaborative planning with hundreds of simultaneous sites interacting as if everyone were across the table will be possible. In addition, fast-forward mission planning and contingency analysis will be routinely used to explore options and novel concepts well beyond human capability.

Another example is automatic target recognition. Image-based ATR is an extraordinarily difficult task, even for highly trained image analysts. It is not surprising that current ATR systems are woefully inadequate. It is not possible to fuse the necessary data in real-time, nor is it possible to apply the levels of computer power required to replicate the skills of a trained image analyst. But by the year 2015-2020, it will be possible to perform many image analyst tasks. ATR with such a capability is a Grand Challenge problem. This, of course, is more than a computing power issue and will require very significant advances in algorithms.

Augmenting Human Intelligence Through "Bootstrapping"

The technological capabilities described above are necessary to make the progress required, but they are not sufficient. One other element needs to be added to facilitate the transformation of data to knowledge: an active program that incorporates the user in those systems so that these tools truly augment human capabilities. To achieve this, both computer and human capabilities must be advanced together. Computers must augment human abilities and users must augment the computer's capabilities. This "bootstrapping" of human and computer capabilities is fundamental if the most meaningful and compelling advances are to be made.

An example of the kind of research and approach needed is that of Doug Engelbart and his team. Almost 30 years ago Engelbart, under funding from DARPA and while at SRI International, conducted basic research on computer systems that would augment human intelligence. At this time, people used punch cards to interact with computers – a very user unfriendly method. When Engelbart presented his work in San Francisco to a group of over 1,000 researchers, he demonstrated the mouse, hypertext, collaborative worksheets, two-way teleconferencing, and much more that is taken for granted about today's PCs. All were working demonstrations. He established, for the first time, a vision where both the computer augmented the human's capability and the user augmented the computer's capability. It was a revelation.

After Engelbart's demonstration in San Francisco, his team received a standing ovation. Later this work became the basis for the PC industry as it is known today. Many people who saw this demonstration consider it to be the single most important demonstration of computer science ideas ever performed. It won Engelbart international recognition and most of the major awards in computer science, including the Turing Award.

The question that needs to be understood, however, is how Engelbart's team achieved that remarkable series of discoveries. He started with a compelling vision of augmenting human capability, which inspired his team. But he also demanded constant iteration and *implementation* of every idea. It was not enough to talk about an idea, it had to be instantiated so one could determine if it would work and truly augment the ability of people to do the task better. His team constantly tried out new ideas and shared them with each other. At the same time, his team (the users) also had their abilities extended as they used and developed each new idea. Thus, there was a mutual bootstrapping of both computer and human capabilities. When done with commitment, this process can result in exponential progress.

The next 20 years will result in technological capabilities far beyond any that Engelbart could envision when he was doing his pioneering work. To take advantage of these developments, his bootstrapping approach must be used. Writing a conventional request for proposal with specific requirements results in linear developments that are often of no compelling use to a user. Engelbart's message remains the model for how to perform research in information technology: focus on what users need by including them constantly in the design process; continuously iterate new ideas; and instantiate all concepts. Advances as significant as Engelbart's are required to create Cognitive C^4. DoD should evaluate its programs and its results against this model.

Web-Centric World

One of the most significant developments in information technology is the Internet. Although the Internet was initiated several decades ago, it is effectively less than five years old and it has already begun to completely transform the way people work and live. The growth of the Internet is unprecedented, with a doubling rate of less than 12 months.

Internet speeds are effectively limited to 10 to 100 kilobits-per-second. By 2010 the average consumer will have access to many megabits-per-second and by 2020 every PC will be able to receive multiple channels of streaming high-definition video at over 20 megabits-per-second. Over this 20-year period, society will continue to transform, as Internet interactions move from email and images to movie-quality video and fully realistic 3D teleconferencing. At the same time, displays will evolve from small 1k x 1k pixel systems to wall-size displays with 10k x 10k pixel resolution or more.

In addition to these capabilities, the consumer and commercial world has an insatiable appetite for portable, high-speed information systems. These include direct-broadcast satellite, VHF and UHF digital video distribution networks, cellular phone and data systems, and new high-speed Local Area Networks (LANs), such as LMDS. At the same time, high-speed wireless LANs within homes and offices are under development. Clearly, this zeitgeist represents the basis for future military communications systems. But it is much more.

N^2 Business Models

Much attention has been directed toward the extraordinary e-commerce companies. These companies are based on new, non-linear communications strategies that are made possible for the first time by the Internet. The task force notes with some concern that an understanding and use of this model is not apparent within DoD.

In order to understand this potential, consider first the invention of the telephone. It represented the ability to communicate from one individual to another. In a sense, its value was "1." The invention of radio was an advance because it allowed broadcasters to communicate with "N" listeners. By analogy, radio's value is proportional to its listener population, "N." Television represented a further advance with the addition of moving images. TV's value is also proportional to "N."

But the Internet is not just a telephone-radio-TV, also with a value of "N." Rather, it is a new medium that allows each person on the grid to broadcast to N people where, in turn, they can broadcast to "N" more. Thus, its value is proportional to N^2. (In principle, this process can continue beyond N^2.) Figure 6 illustrates this concept. Because this communications strategy is non-linear, when it is utilized as the basis for competitive advantage over time, it dominates companies with N-based business strategies. Companies such as Amazon.com, Dell, and HotMail have all learned to employ N^2 business strategies against their competition. For example, building new bookstores is obviously an expensive, N-based strategy.

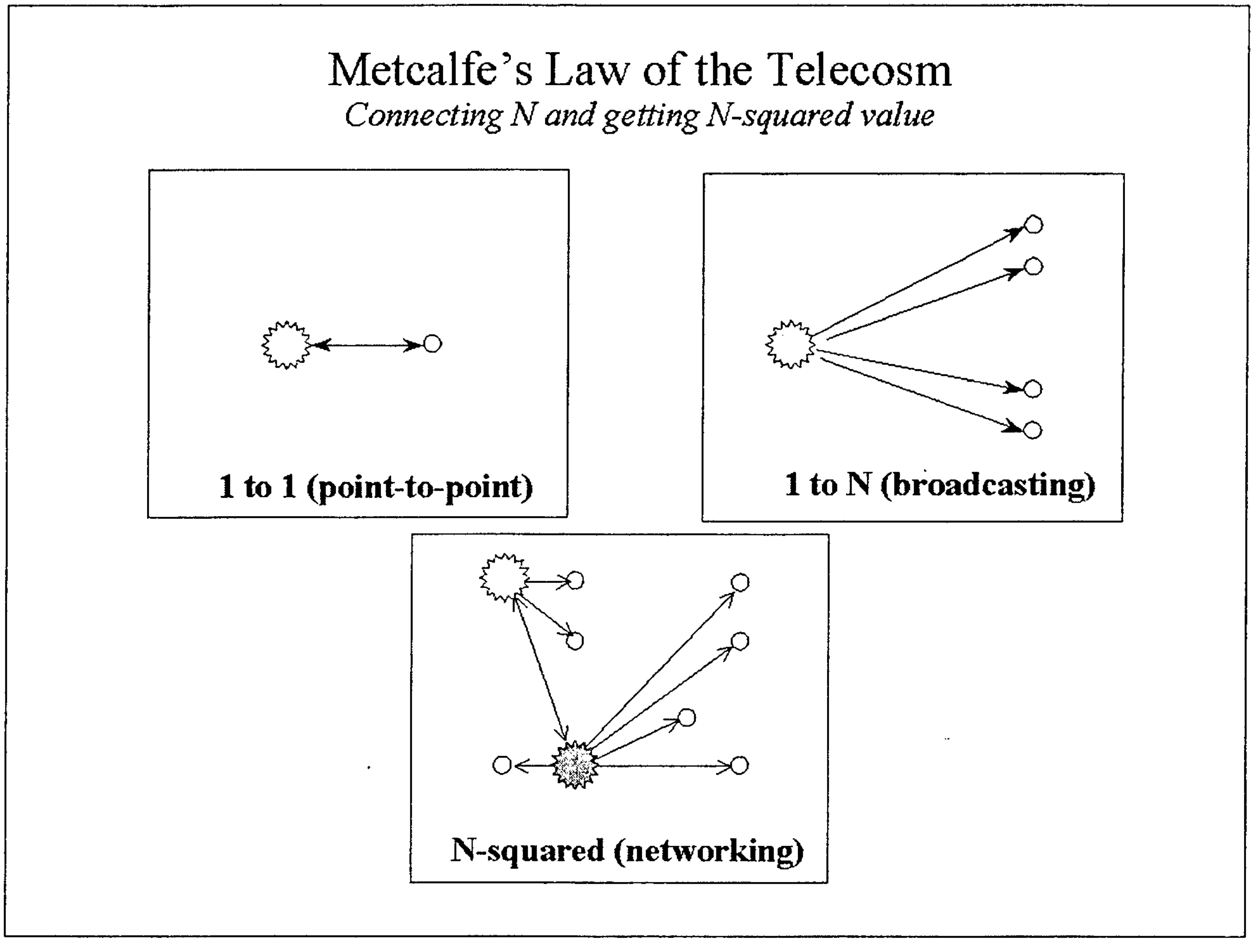

Metcalfe's Law of the Telecosm
Connecting N and getting N-squared value
1 to 1 (point-to-point)
1 to N (broadcasting)
N-squared (networking)

Figure 6: Metcalfe's Law

Why can't DoD begin to employ such powerful models to the way it conducts its operations? At one level, these ideas should be directly applied to logistics and other day-to-day operations of DoD. Enormous savings are possible. At another level, these N^2 concepts must be applied to warfighting. The same competitive advantage exists here as it does in the private sector.

Ubiquitous Computing Environments

As a result of the miniaturization of computer devices, they are becoming embedded in everyday products everywhere. Every product is also becoming a potential node on the web. For example, when commanders walk into a war room of the future, they will have a tag (either worn or embedded) that will identify them to the computer systems distributed in and around the war room. The commander's PC will automatically be connected to a wireless system that will be updated with necessary information at the appropriate security level. By 2015-2020, wall-size electronic displays will be common and speaker-independent, broad vocabulary speech recognition will allow more intuitive forms of communication between the commander and the war room information and decision aids systems.

From Data to Knowledge

Transitions like the one described above will profoundly change the way computer and networking technologies are used. A simple example helps illustrate this point. Consider the following four concepts:

Data **(2000)**	**Information** **(2010)**	**Knowledge** **(2020)**	**Understanding** **(beyond 2020)**

Today, the basic infrastructure to rapidly communicate wide-band data is under development. But the ability to process that data and turn it into useful information is still very limited. Search engines and simple artificial-intelligence agents provide only rudimentary support. Internet searches, for example, often result in thousands of links, but not the information the user is after. By 2010, search tools will be based on speech input, with natural-language search engines that will begin to convert links into useful messages. Increasingly, information will be customized to user needs. By 2020, the availability of high-speed networking and of computers that perform at human equivalent rates will make it possible to convert information into knowledge. At that point, the computer tools will be powerful enough to provide insights and expertise that is beyond ordinary human capacity. Beyond 2020, these capabilities will extend to in-depth understanding of novel, new environments. The challenge over the next 10 to 20 years is to create information systems that fully exploit the inherent capability of human users.

Thus, the task force believes that the next 20 years should be devoted to developing C^4 systems that not only allow secure, robust, wide-band communications and computing, but that also profoundly extend and augment human warfighting capabilities. Extremely high-resolution displays, as well as other sensor modalities that fully engage users' senses, will be available. There will be an unprecedented ability to visualize the battlespace and enemy capabilities, as well as to plan contingencies, employ ordnance, and control the tempo of operations. DoD will have the opportunity to anticipate the actions of adversaries and to conduct appropriate psychological operations while influencing public opinion.

But there is also the possibility that all these new technological capabilities will create a Tower of Babel. Researchers will need to continue the unfinished revolution of Doug Engelbart and develop systems that are as revolutionary as going from punch cards to a mouse-driven PC was 30 years ago.

The following are a few general comments about the major themes of this section. After these comments, the technology roadmap for the Grand Challenge capability of Cognitive C^4 is presented.

Situational awareness. The overall capabilities described above will become the basis for DoD situational awareness. The web will increasingly provide the core technologies to communicate from the commander level down to the individual warfighter. The fundamental issues for DoD will be to develop systems that are interoperable with commercial systems, that provide the necessary multi-level security, and that use new forms of assurance (for example, redundancy and statistical approaches).

Augmenting human capability. Advances in ubiquitous computing will provide core enabling technologies, but DoD will need to develop the tools and environments that are effective for its missions. Advances in decision support, such as ATR, will remain challenging technological problems, but other decision aids, such as fast-forward contingency analysis, will become commonplace.

Mobile Access. Mobility and personalization are major driving forces for the commercial world and provide the basis for DoD needs. Geographically dispersed, mobile forces require the same degree of access to the Internet. Situational awareness is required by forces at all levels to fulfill the vision of forward ground forces who are fewer in number, but who have access to precision fires by reach-back and who can contribute as individual nodes in the overall C^4ISR environment. Commanders need mobile access to information and decision-making aids to free them from the confines of large, static operational centers. The operational centers themselves must be smaller and distributed for survivability, but must be linked via the Internet to provide information and tools to support the staff and commander decision processes. Inherent to these requirements are technologies, such as advanced wireless LANs and advanced antenna technologies, which permit the Tactical Operational Centers to be mobile and to provide command-and-control products to commanders who are themselves mobile.

Assurance. Advances in GPS technology are required to counter jamming and deception in order to assure navigation, precision weapons delivery, and time synchronization of communications and information systems. Communication links must also be assured in non-line-of-sight environments, such as complex urban terrain. These issues remain the primary concern and therefore responsibility of DoD.

Cost and performance. In many of the areas involving Cognitive C^4, the commercial world will drive the core technologies. It is clear that DoD must build on and leverage these developments to provide the maximum performance at the minimum cost. Yet, DoD still tends to prefer building DoD-unique systems with insufficient attention to major developments in the commercial world. Simply working with defense contractors does not mean that DoD is working with the most appropriate or best private sector companies.

TECHNOLOGY ROADMAP

Computing

Today's information economy is a consequence of many factors, but one of the most important is the unrelenting progress in microcomputers. This progress is most clearly expressed by Moore's Law, which states that computing power doubles every 18 months. All of the applications that are described in this section depend on the continuation of Moore's Law up to 2020 and beyond. Such a continuation would increase the performance of computers by roughly 10,000 times, while lowering power consumption (i.e., less than 50 watts) and would put a human equivalent computer on every desktop. The development of alternative technologies that can maintain and extend Moore's Law is a worthy element of a Grand Challenge program. Different approaches should be considered for revolutionary advances in computing, such as those based on nano-technology and biotechnology. This program should focus on demonstrating fundamental capabilities and removing the risk associated with such profoundly new technologies.

In other sections of this report, the importance and impact of biotechnology is described. These technologies will also impact the computing needs described directly above. At the same time, they allow for the possibility of developing carbon-based computers and processes that can be integrated into biological systems to augment their capabilities. An example would be insects that detect pathogenic agents in the atmosphere. Ultimately human augmentation will be possible.

As described above, by 2010 to 2020 the task force envisions an environment where each person and each device is both a computing and a communications node in a networked world. Integrating all of the necessary resources so that they work cooperatively, securely, and robustly is another element of a Grand Challenge problem. Issues such as updating data, maintaining database integrity, enabling the interoperability of different information sources, and securing the appropriate levels of access through the use of complimentary bio-metric identification systems all must work seamlessly for the system to perform. These systems will be developed by the private sector, but DoD has unique requirements in terms of security and applications that must be developed, demonstrated, and understood in the process of exploiting commercial work.

Information Transmission

To effectively communicate appropriate information to both commanders and warfighters, the bandwidth capability of today's systems will need to be expanded 10,000-fold. This will allow high-definition video to be used extensively and other extremely data-intensive applications. In addition, these systems will be based on open Internet protocols that will allow transparent use of both DoD and commercial networks for the transport of data.

Information speeds will increase at exponential rates. Satellite downlinks to homes are already at 400 megabits per second. By around 2010, there will be 10 megabit-per-second Internet connections, and by 2015, such high data rates will be priced within reach of consumers. Again, the commercial and consumer industry will be the drivers and heavy investors in these technological improvements, and DoD will need to partner with these commercial and consumer leaders to ensure that its systems requirements include the latest advances. The Grand Challenge problem for DoD will include getting capabilities to mobile warfighters on the ground.

Assurance

Assurance will increasingly be provided by the redundant use of multiple forms of communication. Systems will be designed to gracefully degrade and to adaptively send that information which is most important first. These redundant systems will have extensive abilities to process and understand the flow of data. They will be self-healing and able to understand attempts to jam, impede, and block their capabilities.

An increasingly important development is the wide use of international standards. The Internet is a classic example. Similar developments are occurring in voice and data communication, video (for example, MPEG-7), and navigation tools for the Internet. The task force envisions a future where these standards are embraced and aggressively implemented by DoD.

Assurance requirements will encompass multi-frequency GPS by 2004 (at least four frequencies). Advanced internal navigation systems should become available by 2008. By 2017-2020, third-generation robust GPS systems should begin to appear. Major commitments by DoD to all three of these areas will be necessary. Both advanced internal navigation systems and a third-generation robust GPS system are absolutely critical for DoD to maintain its military superiority on the battlefield of the future. All of these elements of assurance also properly belong in the Grand Challenge.

Decision Support

Decision support is critical to allow the use of the enormous amount of data that flows from all elements of a battle. Providing a near-real-time planning and execution environment from the commander down to the warfighter will require dramatically new forms of decision support. Today's decision support technologies remain limited and brittle in their application.

To process and take full advantage of this data, it will be necessary to augment human capabilities in profoundly more powerful ways. The task force envisions an environment where speaker-independent, multiple-language voice input and output is commonly available. Ubiquitous computing and communications will allow continuous interaction with commanders. The location and identity of all coalition forces will be known in real-time. Electronic data will be presented in very high-resolution, wall-sized, flat-panel displays. The 10,000-fold increase in computer power will enable powerful capabilities in decision support tools, such as fast-forward contingency planning and execution. These capabilities will exceed the capabilities of even extremely intelligent human beings. DoD will leverage the increasingly high-speed worldwide data-communications system. By 2020, home PCs will be capable of receiving multiple high-definition (20 megabits per second) data streams. This will allow fully immersive systems, including 3D and other photo-realistic mission planning tools.

Useful automatic target recognition systems for decision support are another Grand Challenge technical problem. To fully use the potential of national and operational sensing capabilities, an automated means must be found to augment the capabilities of image analysts.

Unfortunately, full ATR capability requires computer and algorithmic performance that is comparable to human cognitive capability. Thus, a full solution to this problem requires the availability of dramatically more powerfully algorithms and computer speeds well beyond those of humans. Nevertheless, over the next 10-20 years these technical achievements are possible. At the same time, commercial and consumer-based applications for computer vision technologies are beginning to emerge. A new program that leverages these capabilities and extends them to new applications should be a centerpiece of Cognitive C^4.

Interoperability

Interoperability should become less of an issue as international standards are put into place. Standards for Internet, voice, and data communications are being implemented by the commercial and consumer industries. DoD must take advantage of these efforts and leverage its investment by partnering with industry.

In coalition warfare, each country normally speaks a different language. Significant improvement in speech recognition will be available around 2007 as computer speeds and sophisticated algorithms are advanced. Speaker-independent language translation systems will also be available. Integrating DoD systems with coalition systems and worldwide commercial systems is a Grand Challenge problem.

Interfaces

As discussed above, current display and sensing technologies are not matched to human capabilities. For example, displays that are matched to the resolution of the eye would more fully augment human capability. Other sensory systems – equal to the capabilities of the best biological organisms – are also needed. An example would be employing sense of smell for chemical and biological defense by using devices that can sense as well as a dog and convert those signals into a digital stream for transmission and analysis at a remote site. Advances in materials science, micro-technologies, and biotechnology will allow a new generation of display and sensor technologies that can reach these levels of performance. These are all Grand Challenge problems where again DoD can expedite the development of these capabilities by solving many of the critical and risky technology problems while leveraging private sector developments.

Security

Providing secure network and information systems is fundamental to an information technology-based warfighting capability. Today, it is impossible to state with clarity whether DoD networks contain "back doors" or even who all of the network administrators are. DoD systems administrators also rotate jobs every two to four years, which represents a separate family of security issues.

Providing security over DoD systems, as well as over the commercial systems integrated into the DoD system, is another Grand Challenge problem. New approaches are required, such as statistical monitoring, intelligence network monitoring, and network redundancy. Issues of security and network assurance will become centerpieces of the emerging e-commerce industry.

A successful DoD program will leverage these capabilities and add the additional security and performance features needed by DoD, such as multi-level security.

In addition to knowing that the network is secure, one must be confident about the identity of users on the network. Biometric systems will help facilitate secure and easy access to appropriate data at various levels of security. These biometric technologies, which are now just emerging, will be ubiquitous by 2015-2020. These technologies include fingerprint analysis, voice recognition, face recognition, iris identification, and DNA tagging. Iris identification and DNA tagging have the capability of absolutely identifying every person on the Earth. Biometric systems will be augmented by sophisticated electronic tags that will contain detailed user profiles and GPS coordinates to identify the coordinates of all users.

In a world where it is possible to sense, communicate, and present almost unlimited amounts of data, a critical issue becomes that of finding, using, and exploiting that information. More is needed than just better search engines. A new family of "trusted agents" must be developed that understand user needs and that can augment user capabilities. Today, the agent applications that have been developed are simple cartoons of what is required by 2010-2020. It is a Grand Challenge problem to develop agents that have the understanding and capability a warfighter can rely on during stressful situations. This again is an area that will be developed partly by the commercial world because of its e-commerce applications. But DoD can take the lead in developing key concepts and applications that are specific to its needs.

The technological roadmap to accomplish the Grand Challenge technical issues described above is shown in Figure 7. This figure presents the technical achievements necessary to realize the vision of dominant situational awareness, augmented human capability, and mobility, while satisfying the needs for assurance and improved cost performance.

	2000	2005	2010	2015	2020
Computers	Demonstrate biological computer concept	Demonstrate prototype nano-computer	Deploy soft x-ray lithography	Demonstrate 50 watt 10^4 time improvement bio/nano-computer	
Information	Cable "information on demand" at 5Mb/s	20 Mb/s PC Internet	U.S. TV broadcast converted to HDTV at 20 Mb/s	Low-cost, mobile 20 Mb/s Internet	
Assurance	Multi frequency GPS	Hybrid GPS, advanced inertial navigation Statistical redundancy		3rd Generation, low cost GPS & inertial navigation	
Decision Support	Web-based natural language search engines Limited domain mission planning tools	Feature-based ATR "Trusted agent" search and navigation entities Cross domain mission planning tools		Image analyst capable ATR "Alter ego" search and navigation entities Comprehensive war-gaming tools	
Interoperability		Demonstrate comprehensive interoperability with commercial/consumer systems		Full operational, interoperability with coalition systems	
Interface	Berlitz warfighter with limited vocabulary Scalable flat panel displays (10k x 10k pixels)	Ubiquitous computer environments with limited functionality	Multiple language, speaker independent speech recognition Scent recognition with "dog's nose" sensitivity	Ubiquitous computer environments with I/O devices matched to human capabilities	
Security	Multi-level security Statistical monitoring	Wide use of biometrics & embedded watermarks		Full integrated, intuitive multi-level security Self-healing networks	

Figure 7. Cognitive C⁴ Roadmap

INVESTMENT STRATEGY

This section describes criteria for funding Cognitive C^4 Grand Challenges and the resources needed to solve them. It also outlines some of the management considerations that must be addressed.

DoD and Industry Partnerships

It is clearly understood within DoD that private sector information technology investments far outstrip those of DoD. Thus, the central issue is: where should DoD invest its funds to gain the largest military advantage? Clear distinctions must be made for the government to justify its investments. The task force believes that DoD should use the following criteria in making these investment decisions. When used aggressively and with the proper contracting vehicles, these criteria can significantly advance the development of needed technologies, involve the best U.S. intellectual resources, and provide the technology base and DoD systems needed to maintain U.S. warfighting dominance.

1. *Clear military need.* Projects should only be initiated where the impact of the technology will provide a significant military advantage.
2. *Grand Challenge impact.* DoD should invest in areas of high technical risk but great payoff – areas where the private sector would not normally invest. DoD should confront that risk where there is a potential for a breakthrough that could create a significant military advantage.
3. *DoD-unique capability.* In selected technologies, such as ATR, UAVs, and lethal systems, DoD must develop its own technologies and systems.
4. *Criteria for industry involvement.* Beyond the defense contracting community, the private sector will only work with DoD when they see that a technology can have large commercial impact. These dual-use technologies are those where DoD can expect interest from industry, provided that DoD will help underwrite and remove technical risk. In effect, DoD would provide the "courage" for industry to pursue a risky, high-payoff path. DoD should look for these opportunities within the Grand Challenge context. In addition, DoD must use its alternative contracting authority, such as that employed by DARPA, to attract the best commercial resources.

Finally, DoD must learn to more effectively participate in international standards organizations as a partner and co-equal with other organizations. In the past, the government has often acted as an uninformed but authoritarian interloper in these organizations. The government must learn to act like a partner and bring forward its best technical arguments and demonstrations for evaluation and inclusion in the standards.

Roadmap Investment Strategy

The roadmap section above listed several areas of technology development. The following list summarizes the levels of investment recommended for each of the areas discussed above:

- Computing: Human speed, $100M/year
- Information: Global, human-rate communication, $100M/year
- Assurance: Confidence and trust, $150M/year
- Decision Support: Augmenting human capabilities, $100M/year
- Interoperability: Connectivity with everyone, $200M/year
- Interface: Human-matched interfaces, $100M/year
- Security: Trusted environments, $100M/year (to no avail)
- DoD N^2 Strategic Research Strategies, $100M/year
- *Other* research strategies (see below), $10M/year

The task force recommends that DoD develop pilot programs that emulate the research methodology pioneered by Doug Engelbart when he invented the mouse and other core technologies that are now the basis for the modern PC. This methodology is the most powerful means of building information systems that are compelling and that augment human intelligence. The task force recommends that DoD establish an institute based on these principles to highlight and promulgate this methodology throughout DoD. Recommended funding is $10 million per year.

S&T MANAGEMENT, INVESTMENT STRATEGY

ISSUES

Figure 8 below lists some of the more pressing issues concerning DoD science and technology and acquisition programs, as outlined by recent Defense Science Board task force reports.[1] These same points have been mentioned repeatedly in many other studies on this subject that have been undertaken in recent years – the most recent being an Air Force study of their laboratories entitled "Workforce 21 – Options for a 21st Century S&T Workforce" by Dr. Daniel Hastings, AF/ST.

- S&T program not sufficiently focused on technology offering order-of-magnitude increases in U.S. military capabilities.
- Current Service S&T management and execution are generally judged not to be up to industrial or university standards.
    - Civil-Service Personnel System problems
    - Facilities are generally not up-to-date
    - Technical support very limited
- Experimental field testing of revolutionary military capabilities is very limited.
- Acquisition of test and initial capability systems is slow and difficult because of the use of 5000.1 and Federal Regulations, instead of modern commercial practices.

Figure 8 S&T and Acquisition Issues

These various topics will be treated below, but first the principal points of an S&T and acquisition strategy will be discussed.

S&T AND ACQUISITION STRATEGY

The objective of an S&T and acquisition strategy is to maintain and increase the military advantage of U.S. forces. This topic is outlined in Figure 9 below. Basically, this recommended strategy calls for a new emphasis in three areas.

1.

[1] Report of the Defense Science Board task force on Defense Science and Technology Base for the 21st Century, June 1998.

- Focus major part of S&T program management and execution on technology advances which can lead to major (>10:1) advances in U.S. military
  - Exploration of new technologies
  - Exploration of advances in current technologies which are beyond the time horizon of commercial R&D (1-5 years)
- Iterative field-test of military capabilities incorporating advanced technologies and tactics using fast (commercial) design and manufacturing processes with experimental military test forces.
- Acquisition of initial revolutionary military capabilities using commercial acquisition practices. When proven in experimental military use, acquire such capabilities for the rest of the forces.

Figure 9: S&T and Acquisition Strategy

Discussion of Options

S&T Program Focus

As pointed out above, the S&T strategy calls for an emphasis on developing military capabilities that offer large advantages over current systems. Figure 10 outlines three possible options for achieving this end.

The first option is to continue with the current portfolio of technology efforts. This portfolio does indeed support such technologies to some extent. Portions of the DARPA program and, to a lesser extent, those of the military Services are aimed at such advances. However, the totality of these efforts probably constitutes only 10 percent of the total S&T effort. The rest of the program is focused on incremental improvements to current defense systems, which are important but which consume an excessive amount of the total S&T program.

The second option suggests that at least one-third of the S&T program should be devoted to what are called Grand Challenge technology programs. These would be efforts ranging from basic science to prototype demonstrations that promise large gains in future U.S. military capabilities. One-half to two-thirds of the S&T program would still be devoted to incremental improvements in current systems. This option is the focus of the S&T program direction recommendation.

	OPTION	PRO	CON
	Current Portfolio: Focuses mostly on incremental improvements in U.S. military capability	Least disruptive to current program	Mostly not focused on order-of-magnitude advances
➡	1/3 of S&T program focused on Grand Challenges offering 10:1 advances in U.S. military capability	Offers the potential for large advances in U.S. military capability	Requires new staff, facilities and programs
	Entire S&T program focused on Grand Challenges	Maximizes long-term U.S. military capabilities	Short-term incremental advances in current U.S. military systems are neglected

Figure 10: S&T Program Options

The third option would be to devote all of the S&T effort to Grand Challenge programs. This degree of concentration on the more distant future would be unwise since current systems can be significantly improved using incremental advances, thus improving U.S. military capabilities in the nearer term.

S&T Management

The current DoD S&T management structure consists of five principal components: an OSD component, DARPA (which reports to OSD but which is quite separate), and separate S&T management organizations in the Army, Navy and Air Force. The Director, Defense Research and Engineering (DDR&E) carries out an overall review of these separate efforts. Despite the heavy burden of this review, DDR&E generally does not exercise much direction in the size and scope of the separate service programs.

Staffing of the Service and OSD S&T management organizations is generally comprised of long-tenure Civil Service personnel. The relatively low turnover of these staffs tends to inhibit the introduction of new ideas into the S&T programs. Most industrial organizations, for example, have found it important to rotate managers among different areas at intervals of four to six years; after that interval of time, most individuals have brought forth most of their ideas for new research or technology directions in a particular field.

In the case of DARPA, an unusual technical management organization is employed, which is generally recognized as providing dynamic and creative direction for the DARPA programs. Somewhat more than half of DARPA's management staff is temporary assignees from outside the government. They are drawn from the leading U.S. research universities and industrial laboratories. The rest of the staff comprises term duty military officers and a smaller number of longer tenure civil servants. Figure 11 indicates several possible options for future DoD S&T management.

	OPTION	PRO	CON
	Current combination of OSD and Service, mostly civil servant organizations, plus DARPA with mixed IPA, military, civil servant staffing	Least disruptive	Dispersed management between Services and OSD. Except for DARPA, lack of staff turnover inhibits development of new programs offering order-of-magnitude improvements in U.S. military capabilities
➡	Employ DARPA-like management structures in Services and OSD	Greatly enhances probability of programs offering breakthrough advances in U.S. military capabilities	Requires new type of staff personnel system which emphasizes 4 to 8 year appointments using IPAs for more than 50% of staff
	Consolidate all S&T management in OSD	Provides strong central control	Greatly restricts possibility of alternative sources for funding new ideas
	Employ private firms to manage S&T programs	Should enhance breakthrough advances if high-quality staff is available	Inherent government function is outsourced

Figure 11: S&T Management Options

The first option is to continue the current S&T management arrangement. This option would offer the least disruption, but it would not energize the program with new directions beyond that provided by DARPA.

The second option would use the DARPA model for the Service and OSD S&T management. This option would require significant modification of the current organization, and a significant amount of staff turnover would result for employing temporary scientific personnel from the private sector for well over half of the management staff. Separate Service, DARPA, and OSD S&T management organizations would continue to provide alternative sources for support of new concepts. Much stronger management is envisioned for DDR&E which would insure that the overall program was sufficiently focused on major advances in future U.S. military capabilities and that, when necessary, competition is employed to insure success in the various programs. This is the option chosen in the recommendation concerning S&T management.

The third option is to consolidate all S&T management in a single OSD organization. This option has the advantage of strong control, but it has a severe defect in that it eliminates all possibility of alternative sources of funding for new defense technology ideas. As an example, it is doubtful that high-temperature superconductivity would have been found if IBM had all its research in a single laboratory under tight control.

The fourth option is to employ private sector management of DoD and Service S&T programs. This option has the potential to generate programs focused on break-through technologies; if high-quality staff is employed and turnover is significant. The issue with such an arrangement is that inherently governmental functions will be exercised by a private sector organization, which can raise a number of problems. It will be interesting to see how the UK military handles these problems with the "privatization" of its R&D organization.

Service Laboratory Capabilities

A large number of studies of the Service laboratories have been carried out over the past few decades. These studies generally have indicated that the Service laboratories are not competitive with leading industrial and university laboratories in terms of innovation and technical leadership. Other measures also indicate substantial differences. For instance, an examination of the memberships of the National Academy of Science and the National Academy of Engineering indicates that very few members come from DoD laboratories in comparison with industrial and university laboratories. The same difference is noted upon examination of patent citations to scientific and engineering papers published by various laboratories. Annexes C and D provide data supporting this observation.

A notable exception to this general observation is the Naval Research Laboratory. A few other defense laboratories also have good records of accomplishment in selected specialized fields.

Most studies of this problem have noted that the structure of the Civil Service Personnel System makes it difficult for DoD laboratories to recruit and retain highly qualified staff. During and just after World War II, these laboratories recruited many capable staff, some of whom are still with them. However, in recent years, the civil service salary structure has fallen significantly behind the market for talented technical staff. In addition, performance review processes generally do not reward the best performers with adequate salary increases and promotions to close the gap with the market for skilled professionals. At the same time, civil service policies make it extremely difficult to discharge staff whose technical performance is inadequate.

In addition to problems with personnel policies, most DoD laboratories have drastically reduced technical support to the professional staff. Under budget pressures, coupled with the excessive size of the aggregate DoD laboratory work force, the internal technical work has diminished in favor of outsourcing with the resulting technical atrophy of the staff. Finally, in some cases the research facilities have not kept up with those of industrial and university laboratories. Figure 12 indicates three options for coping with the problems cited above.

OPTION	PRO	CON
▪ Modify current Civil-Service personnel system for laboratory staff	▪ Least disruptive	▪ Unlikely to be able to recruit and maintain outstanding staff because salaries are not competitive, promotions limited, and discharge of unsatisfactory staff is nearly impossible
➡ ▪ Use private sector (universities & industry) to supply professional staff, top leadership to be provided by SES government personnel. Current Civil-Service staff retire when they wish. Laboratory size maintained	▪ Recruits and maintains outstanding staff using university or industrial personnel practices	▪ Requires time and transition to mostly private sector
▪ Outsource entire laboratory function to private sector. (University or industrial organizations)	▪ Rapid transition to high-quality staff	Private sector executes inherently government functions. Rapid displacements of Civil-Service staff may lead to political problems.

Figure 12: S&T Laboratory Options

The first option involves drastically modifying the current civil service personnel system, along with significant improvements in the areas of technical support and facilities.

There have already been several attempts to modify the civil service system. Most observers, including several current Service laboratory directors have reported that these changes are inadequate and do not address the fundamental problems. They believe that even with these changes, they will be unable to successfully compete for the skilled technical staff that they need.

The second option is to staff these laboratories with professional staff provided by the private sector, primarily from universities and industrial laboratories. The private sector organizations would be the employer of these individuals, who would be paid at current market rates and rewarded in proportion to their accomplishments. Fairly regular turnover would be achieved as these individuals return to their parent organization after several years. Current civil service staff would be allowed to continue until their retirements. In this manner, a smooth transition would be achieved over a number of years.

Leadership of the DoD laboratories would remain with DoD in the form of the Senior Executive Service personnel who might be recruited from the staff provided by the private sector. In this way, important government functions would remain within the government. This second option is the recommended one.

The third option would be to outsource the entire laboratory function to the private sector. This option has the potential to recruit a highly qualified staff. However, it does not solve the problem of the current civil service laboratory staff and it raises the question of whether a private organization should perform government functions.

Acquisition of Advanced Military Capabilities

It is not sufficient just to solve the problems in the S&T system. The acquisition system must also be able to respond promptly to major advances in military systems. Currently, the major advances often fail to transition from the S&T system into acquisition programs and those that do make the transition are often plagued by excessive time delays. Once into an acquisition program, many years may elapse before equipment is fielded and forces are trained to use it successfully. A number of options exist to solve this problem. Figure 13 outlines three possibilities.

	OPTION	**PRO**	**CON**
	▪ Current acquisition system	▪ System in-place and operating	▪ 15-20 years acquisition
	▪ Advanced Concept Technology Demonstration	▪ Brings new concepts to test in a few years outside of 5000:1 and the Federal Acquisition Regulation (FAR)	▪ Does not produce and support useful numbers of equipments with a combat unit to create advanced warfighting capabilities
➡	▪ Uses commercial industrial management, design, and non-FAR contracting	▪ Rapid design acquisition, testing and initial operational capability at lower costs that 500:1 system under FAR contracts	▪ Requires approval for use of non-FAR contracting

Figure 13: Acquisition Options for Advanced Military Capabilities

The first option involves continuing the current system, with modifications to try to effect higher probabilities of transition and shorter acquisition times. This is basically what is going on at this time. This option has the advantage that it does not disrupt the current acquisition system, but it fails to address the problem.

The second option is to continue to use the Advanced Concept Technology Demonstration Program to improve technology transition. This program basically brings new concepts to field trials and is supposed to leave behind equipment that could be used for an initial operational capability. Unfortunately, enough equipment to obtain a meaningful operational capability is seldom procured because of insufficient funding. In addition, long-term maintenance of the equipment and the training of forces are usually lacking. Many good capabilities have been demonstrated under this program, but transition to an advanced military capability often fails to occur.

The third option would provide funding from OSD to ensure the advanced capability is rapidly transitioned to testing and demonstration. It would also provide funding to acquire enough equipment to produce a meaningful initial capability and to train a military unit that could provide an initial capability. Procurement of demonstration equipment and the equipment to outfit an initial military capability would occur using commercial acquisition practices. Outfitting of the rest of the force with this new capability could occur using the normal acquisition process.

The advantage of this option is that it increases the probability of successful transitions, as well as the speed with which an initial operational capability could come to fruition. The disadvantage of this option is that agreement would probably have to be obtained from the Congress to utilize this process. Given the recent proliferation of advanced military technology to potential aggressors, it may be vital to utilize this third option to maintain U.S. military dominance. This third option is the one recommended.

RECOMMENDATIONS

Figure 14 summarizes four recommendations based on the options discussed above. Only the essential points are outlined. Obviously, more details would have to be settled to implement these recommendations. The essential point of the recommendations is that certain changes to the S&T and acquisition programs are necessary if the capabilities of U.S. military forces are to be kept dominant over the next several decades.

Recommendations

Under Secretary of Defense for Acquisition and Technology should:

- Gain Secretary of Defense support for strong control of R&D funding the Under Secretary of Defense of Acquisition and Technology
- Commit a major fraction of the S&T budget (1/3 to 1/2) to provide complete technology solutions to warfighters for a few urgent grand military challenges
- Focus on four critical grand challenges with a major emphasis on the first two
  - "Nowhere to Hide" - Deny enemy hiding
  - "Bio Shield" - Protect the force against biological threats
  - "Cognitive C^4" - Cognitive data processing for target identification and battle planning support of military commanders
  - "Fast Forward" - Rapid deployment of overwhelming combat forces
- Staff the preponderance of Service S&T management and execution organizations with
- Scientists and engineers on term appointments from universities and private industry
- Establish the ability to obtain initial military capabilities employing critical new technologies through the use of rapid industrial contracting practices.

Figure 14: Recommendations for S&T and Acquisition

ANNEX A. TASK FORCE MEMBERSHIP

Co-Chairmen

Ken Gabriel	Carnegie Mellon University
Walter E. Morrow, Jr.	MIT Lincoln Labs

Executive Secretary

Dick Urban	DARPA

Task Force Members

Ivan Bekey	Bekey Designs
Denis Bovin	Bear, Stearns & Co. Inc.
Curt Carlson	SRI International
Bob Colwell	Intel
Darryl Greenwood	MIT Lincoln Labs
Bill Howard	Consultant
Ira Kuhn	Directed Technologies, Inc.
Reuven Leopold	Syntek Technologies, Inc.
Ed Marram	Geo-Centers, Inc.
George Poste	SmithKline Beacham
David Shaver	MIT Lincoln Labs
Victor Weedn	ADFS

Advisors

William Berry	AFRL
Maj Stephen Kirkpatrick	USMC
Bob Kolesar	Joint Staff, J-8
Ed Mazannti	TRADOC
LtCol Richard Moore	AFRL
Rick Morrison	OAS Army for RD&A
RADM Charlie Young	Naval Sea Systems Command
CDR Randy Young	Joint Staff, J-8

DSB Secretariat

LTC Don Burnett	USA
LTC Scott McPheeters	USA
Christopher Bolkcom	SAIC

ANNEX B. TASK FORCE TERMS OF REFERENCE

DEFENSE TECHNOLOGY STRATEGY AND MANAGEMENT

This task force will interact with the other three task forces to identify and examine a wide range of technologies. The goal is to identify those technologies with high potential to enable the development of unique and superior operational capabilities in 2010 and beyond. This task force will also develop a road map and investigate recommendations to ensure that the DoD is able to always retain an affordable force capability in the 21st century that is well matched to the foreseeable needs and that DoD retains the ability to surge with the greatest capability if and when necessary. Recommendations on technology policy, management, acquisition, and use of commercial technologies will also be developed.

ANNEX C. NATIONAL ACADEMY MEMBERSHIPS IN UNIVERSITIES, INDUSTRIES, NATIONAL LABORATORIES, AND GOVERNMENT LABORATORIES

The following figures list the number of members of the National Academy of Science and the National Academy of Engineering in four classes of organizations:

- Universities
- Industrial Laboratories
- National Laboratories
- Government Laboratories

For compactness, universities with less than 13 members are not listed. For the other organizational classes, memberships of less than three are also not listed. It should be noted that very few of the military service laboratories are listed. A notable exception is the Naval Research Laboratory.

University	Total Membership	University	Total Membership
Mass. Institute of Technology	184	University of Michigan	29
University of Cal. Berkley	170	University of Pennsylvania	29
Stanford University	157	University of Southern Cal.	28
University of Cal. Santa Barbara	127	Northwestern University	25
Harvard University	119	Purdue University	21
Cal. Institute of Technology	84	University of Cal. Davis	20
Cornell University	63	University of Colorado Boulder	20
Princeton University	56	Pennsylvania State University	19
University of Illinois	55	Rice University	18
University of Cal. San Diego	54	Rutgers University	18
University of Wisconsin	53	University of Cal. San Francisco	18
University of Texas	51	Georgia Institute of Technology	17
Yale University	49	University of Cal. Irvine	17
University of Cal. Los Angeles	42	North Carolina State University	16
University of Utah	35	Johns Hopkins University	15
Columbia University	34	Carnegie Mellon	15
University of Minnesota	31	University of North Carolina	14
		University of Maryland	13

*National Academy of Sciences and National Academy of Engineering

Figure 15: National Academy Membership at Leading U.S. Universities

Industry	Total Membership	Industry	Total Membership
IBM Laboratories	43	Hughes Aircraft Company	6
Bell Laboratories - Lucent	41	Xerox Corporation	6
AT&T Bell Laboratories	27	Raytheon Company	5
Lockheed	27	Sarnoff Laboratory (RCA)	5
TRW	19	3M	5
GE Company	13	Chevron Corporation	5
Dupont	11	Bechtel Group	5
Ford Motor Company	9	Mobil Research & Development Corp.	4
Hewlett Packard	9	Chrysler Corporation	4
Northrop Corporation	8	Varian Associates	3
Intel Corporation	7	Motorola, Inc.	3
Exxon	7	Comsat Corporation	3
Microsoft Corporation	7	Honeywell	3
United Technologies	6	Rockwell International Corp.	3
Merck	6		

*National Academy of Sciences and National Academy of Engineering

Figure 16: Industrial Members of National Academies

National Laboratories **	Total Membership	Government Laboratories **	Total Membership
Scripps	22	→ Naval Research Laboratory	6
Brookhaven National Laboratory	12	NASA Langley Research Center	6
Argonne National Laboratory	9	Department of the Navy	5
Sandia National Laboratories	8	NIST	5
Oak Ridge National Laboratory	8	NASA Ames	3
Lincoln Laboratory	7	NASA Goddard	3
Lawrence Berkeley	7	NASA Johnson	3
Los Alamos National Laboratory	6	Department of the Air Force	3
Jet Propulsion Laboratory	5	DoD OSD	3
Southwest Research Institute	4	U.S. Army Corps of Engineers	3
Draper Laboratory	3		
Fermi National Accelerator Laboratory	3		
Illinois Institute of Technology	3		

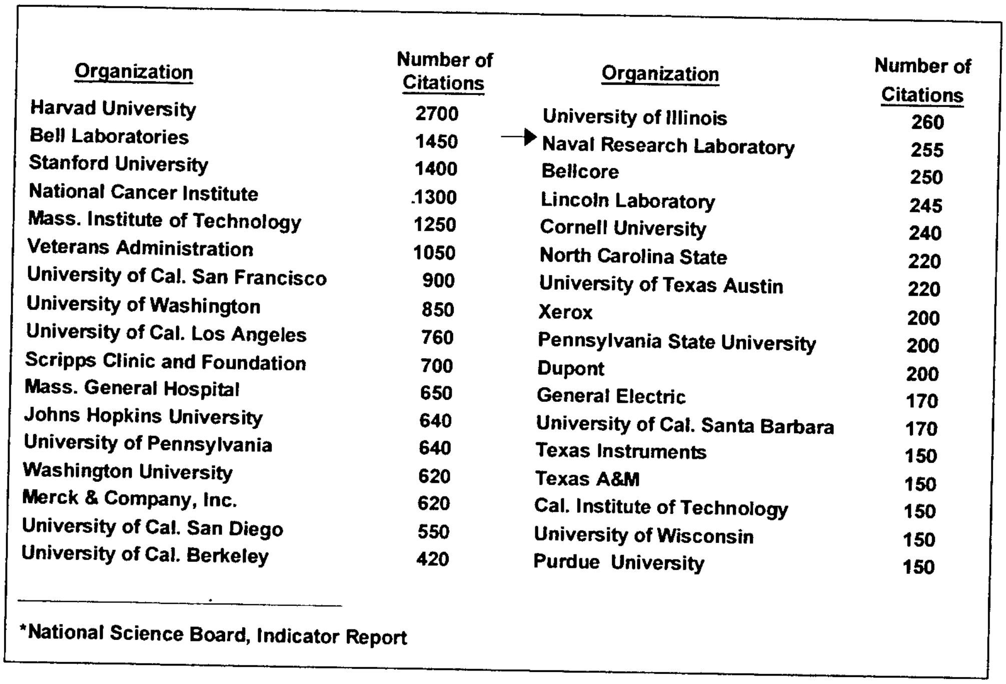
*National Academy of Sciences and National Academy of Engineering
**Non-profit, URACs, FFRDCs,GOCOs

Figure 17: National Laboratories and Government Members of National Academies

ANNEX D. U.S. PATENT CITATIONS OF RESEARCH PAPERS FROM TOP RESEARCH INSTITUTIONS, 1993-1994

The following chart shows the number of citations in patents issued in 1993 and 1994 of research papers from the organizations listed. Such citations are a powerful indicator of technology transfer to commercial applications.

Note that only the Naval Research Laboratory, among all the military service laboratories, is cited in this list of leading research organizations.



Organization	Number of Citations	Organization	Number of Citations
Harvad University	2700	University of Illinois	260
Bell Laboratories	1450	→ Naval Research Laboratory	255
Stanford University	1400	Bellcore	250
National Cancer Institute	.1300	Lincoln Laboratory	245
Mass. Institute of Technology	1250	Cornell University	240
Veterans Administration	1050	North Carolina State	220
University of Cal. San Francisco	900	University of Texas Austin	220
University of Washington	850	Xerox	200
University of Cal. Los Angeles	760	Pennsylvania State University	200
Scripps Clinic and Foundation	700	Dupont	200
Mass. General Hospital	650	General Electric	170
Johns Hopkins University	640	University of Cal. Santa Barbara	170
University of Pennsylvania	640	Texas Instruments	150
Washington University	620	Texas A&M	150
Merck & Company, Inc.	620	Cal. Institute of Technology	150
University of Cal. San Diego	550	University of Wisconsin	150
University of Cal. Berkeley	420	Purdue University	150

*National Science Board, Indicator Report

Figure 18: 1993-1994 U.S. Patent Citations of Research Papers from Top Research

PART IV. STRATEGIC AGILITY

INTRODUCTION

Strategic agility is the ability to rapidly employ joint forces when and where they are needed and to maneuver them within the theater as required to decisively dominate the battlespace. The United States needs such capabilities to get into the battlespace before the enemy "sets" the conditions. The nation needs to be able to generate enough combat power and arrive fast enough so that a credible conventional deterrent is presented to a thinking enemy. If deterrence fails, ensuing operations by both early entry and follow-on forces will be required to terminate the conflict under circumstances favorable to the United States and its allies.

Achieving strategic agility involves changing processes and major event time-lines. There are also a myriad of movement and support issues that are important, such as strategic lift and port issues. Solving these concerns, however, will not solve the United States' strategic agility deficiencies unless joint force elements are also improved.

Strategic agility is needed for all elements of the joint force. DoD general purpose forces, with some exceptions (long range bomber and sea launched cruise missiles), have a modest range of action when compared to the distances that can be achieved with strategic power projection (~ 3000 to 8000 nautical miles) or theater operations (500 to 2000 nautical miles). As an example, tactical air forces operate most efficiently and effectively when their bases are proximate to combat and target locales (~300 nautical miles). These ranges can be extended with extra fuel tanks and tankers with less efficiency and presence. In early entry circumstances, building up more assets in forward areas takes more time and more lift assets, which are already over-stressed.

Analogous characteristics apply to the Army, the Marines, and Naval aviation. Proximity is important in that it constrains an opponent in all domains leaving no real options to escape the presence and effects of U.S. military power. Therefore, gaining assured access and proximity is crucial for the early entry force.

Because of the complexity of joint operations, this report presents examples of operational challenges to structure rationale and recommendations for improving strategic agility. Emphasis is given to Army and Marine examples because establishing these forces assuredly and early is more complex than sea basing or basing theater air forces. In addition the Army establishes theater support for other Services which adds to the complexity of its operations.

Establishing proximate air bases and sea forces is also a challenge but is not treated in this chapter. The matters treated and solutions proposed are judged to be beneficial to all joint force elements.

THREATS AND CONCEPTS

There is a growing consensus that future threats will be different from those of the past. The spectrum of threats will be greater and will require a broader range of U.S. capabilities.

In the past, the United States planned its forces to offset the threat posed by the Soviet Union. Marginal superiority was sought in critical areas. Forward basing, theater prepositioning, and reinforcement provided hedges. All other threat circumstances were judged to be lesser-included cases and required little or no special treatment.

Possibly the most insightful characterization of the future threats has been to establish the idea that there is no single overriding and central threat. Preparing for one, assuming all others to be included cases, is a poor starting point. In addition, asymmetric threats enhance the threat challenge.

In this period of both uncertainty and preparedness, the Joint Chiefs of Staff and the Services have embarked on future force planning to underwrite a national strategy of prepare, shape, and respond. *Joint Vision 2010* is the overarching vision for the future. It posits dominance in all phases of future operations, particularly in the critical domains of power projection, sustainment, force protection, engagement, and maneuver. These, built on a base of high quality leaders and soldiers and superb training, should both enhance deterrence and produce more favorable engagement and campaign circumstances than in the past.

The Services have embraced this vision in their "flagship" efforts such as Air Force Air Expeditionary Forces (AEF), Marine Corps Operational Maneuver from the Sea and Army AA2010 Army After Next. Shaping subordinate processes and programs is now underway. Thus, research, development, and acquisition efforts in the Services as well as those of Joint activities such as the U.S. Transportation Command (TRANSCOM), have been engaged in the search for means and technologies to underwrite the six central capabilities which comprise *Joint Vision 2010.*

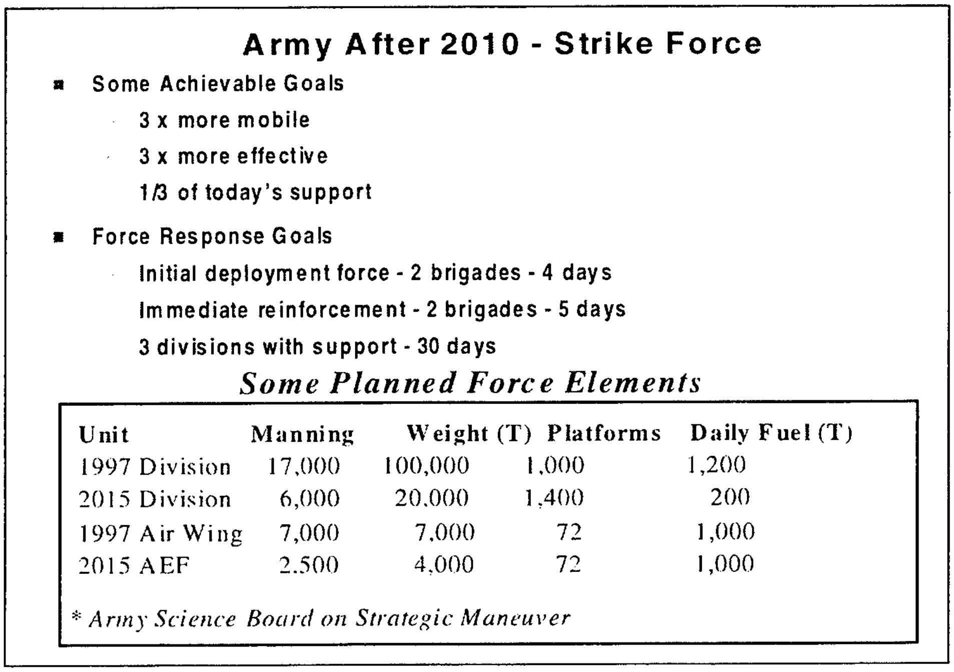
The next section discusses Service concepts for future forces. Ongoing force design efforts will ultimately address strategic agility in an end-to-end context. This report suggests a comprehensive early entry and immediate follow-on force joint warfighting capability assessment (JWCA) as a mechanism to stimulate end-to-end thinking, innovation, planning, and ultimately resource allocation. An example of an end-to-end assessment conducted by the Army Science Board is included as an appendix.

SERVICE CONCEPTS FOR FUTURE FORCES

ARMY

The Army Strike Force concept is designed to make the Army a more agile, deployable force, while retaining the Army mission to be the force that ultimately wins wars and is the most powerful conventional deterrent.

The Army Strike Force consists of a new type of "heavy force" that is lighter and more mobile, as well as a new type of "light force" with increased agility. It also provides for a special type of "strike force" that is three times more mobile and three times more effective in combat power than today's forces.



Army After 2010 - Strike Force

- Some Achievable Goals
  - 3 x more mobile
  - 3 x more effective
  - 1/3 of today's support
- Force Response Goals
  - Initial deployment force - 2 brigades - 4 days
  - Immediate reinforcement - 2 brigades - 5 days
  - 3 divisions with support - 30 days

Some Planned Force Elements

Unit	Manning	Weight (T)	Platforms	Daily Fuel (T)
1997 Division	17,000	100,000	1,000	1,200
2015 Division	6,000	20,000	1,400	200
1997 Air Wing	7,000	7,000	72	1,000
2015 AEF	2,500	4,000	72	1,000

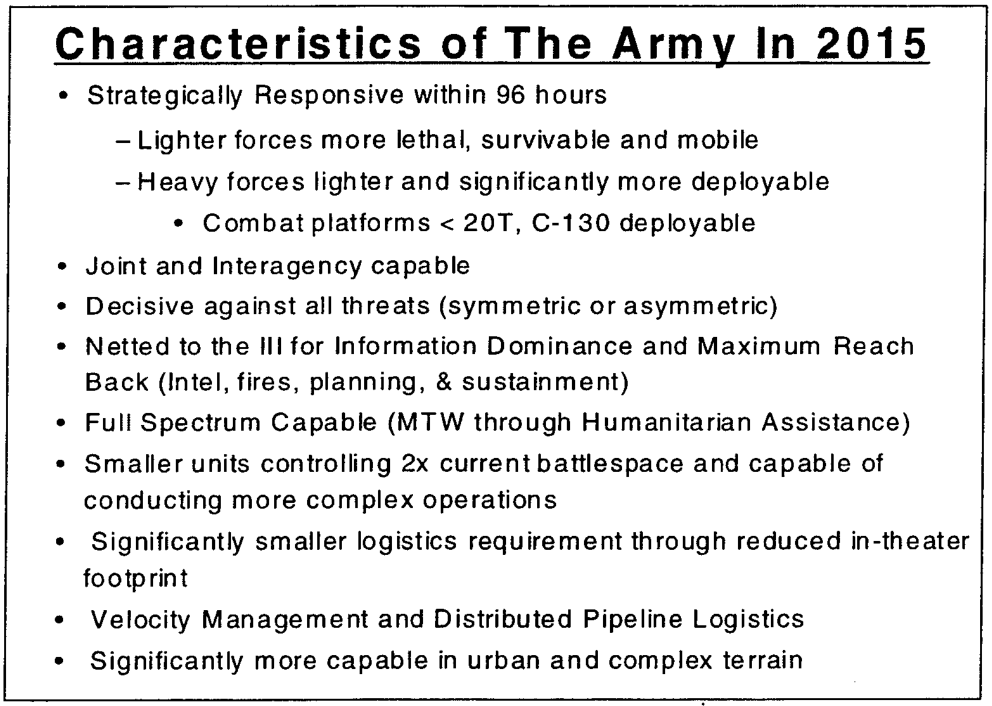
* *Army Science Board on Strategic Maneuver*

Figure 1. Army Strike Force

The Army of 2015 will be strategically responsive within 96 hours, with lighter forces that are more lethal, survivable, and mobile. The Army's heavy forces will be lighter and significantly more deployable (combat platforms < 20T, C130 deployable) as well. These forces will be designed to interface with other Services as a part of a joint force, including forces that are interagency capable.

Army combat power will be decisive against all threats, symmetric or asymmetric, and will be able to respond to the full-spectrum of threats from major theater war to humanitarian contingencies. Smaller units will be able to control significant multiples of the current battlespace and will be capable of conducting more complex operations. Future Army units will be significantly more capable in urban and complex terrain as well.

Forces will be netted to the Joint Integrated Information Internet (JI^3) for information dominance and maximum reach-back (intelligence, fires, planning, and sustainment). Units will have significantly smaller logistics requirements as well as reduced in-theater footprint. The Army logistic system will be based on the Joint Logistic System, as well as velocity management and distributed pipeline logistics.



Characteristics of The Army In 2015

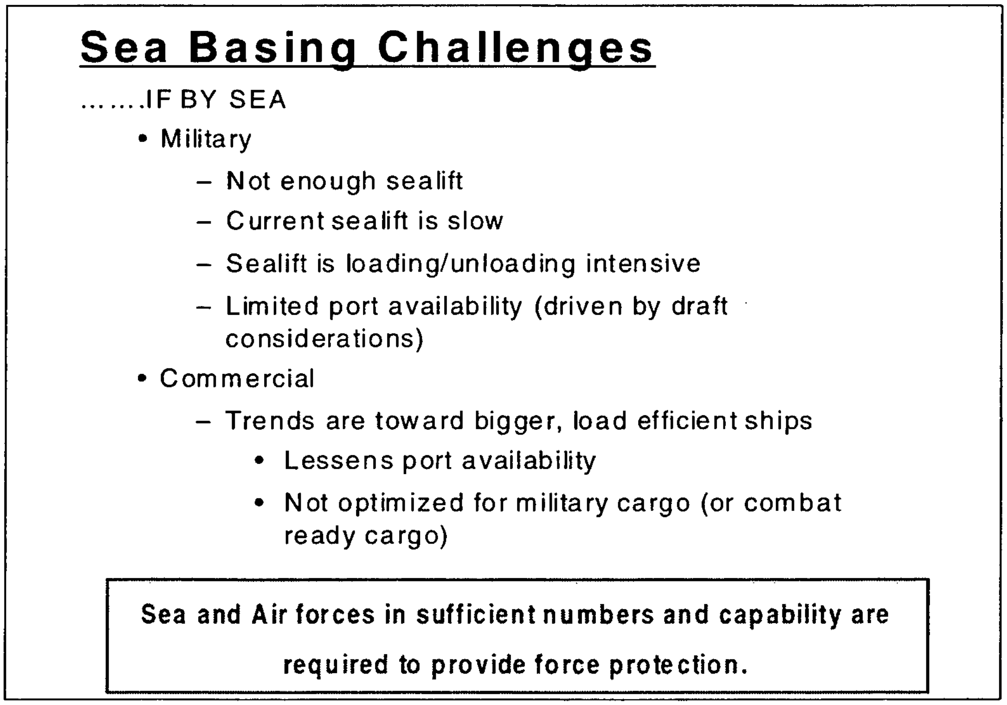
- Strategically Responsive within 96 hours
  - – Lighter forces more lethal, survivable and mobile
  - – Heavy forces lighter and significantly more deployable
    - Combat platforms < 20T, C-130 deployable
- Joint and Interagency capable
- Decisive against all threats (symmetric or asymmetric)
- Netted to the III for Information Dominance and Maximum Reach Back (Intel, fires, planning, & sustainment)
- Full Spectrum Capable (MTW through Humanitarian Assistance)
- Smaller units controlling 2x current battlespace and capable of conducting more complex operations
- Significantly smaller logistics requirement through reduced in-theater footprint
- Velocity Management and Distributed Pipeline Logistics
- Significantly more capable in urban and complex terrain

Figure 2. Army Underwriting Joint Vision 2010 and Beyond

NAVY

Future naval forces will be capable of providing early force protection to arriving air and ground forces, including the ability to break through sea and littoral asymmetric defenses that an enemy can mount. “Minimum footprint ashore” implies a higher degree, at least initially, of basing at sea. Sea-basing challenges include both military and commercial concerns:

- Military
  - Not enough sealift
  - Current sealift is slow
  - Sealift is loading/unloading intensive
  - Limited port availability (driven by draft considerations)
- Commercial
  - Trends are toward bigger, load efficient ships
  - Lessens port availability
  - Not optimized for military cargo (or combat ready cargo)



Sea Basing Challenges

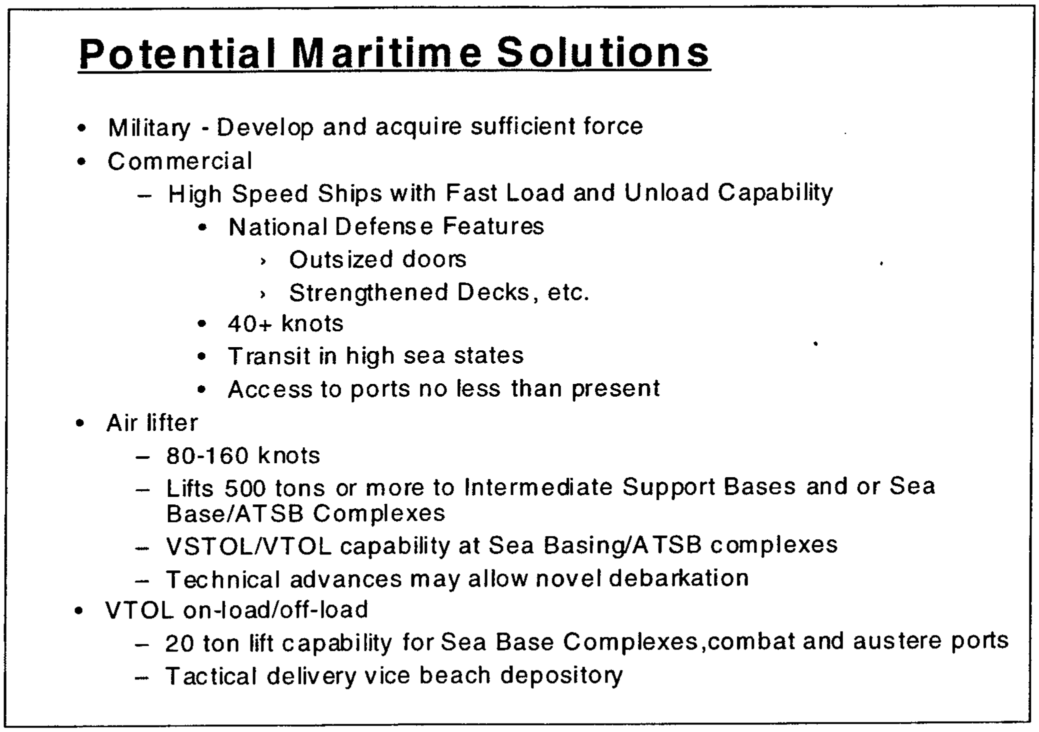
…….IF BY SEA

- Military
  - Not enough sealift
  - Current sealift is slow
  - Sealift is loading/unloading intensive
  - Limited port availability (driven by draft considerations)
- Commercial
  - Trends are toward bigger, load efficient ships
    - Lessens port availability
    - Not optimized for military cargo (or combat ready cargo)

Sea and Air forces in sufficient numbers and capability are required to provide force protection.

Figure 3. Navy Underwriting Joint Vision 2010 and Beyond

Potential maritime solutions considered are many. The Navy can develop and acquire sufficient force for sea basing and forces that can push back asymmetric and other littoral defenses and protect sea basing, sea-based aircraft, and amphibious forces. In the commercial area, an option is to identify additional high-speed ships with fast load and unload capability and invest in building national defense features such as outsized doors or strengthened decks. These ships would be capable of speeds of at least 25 knots sustained, with a goal of 40+ knots. They would be able to sustain such speeds in high sea states – up to sea state 5 – and be accessible to drafts up to 40 feet. The Navy, along with the Air Force is looking into hybrid sea/air lifters that compromise between speed and payload. Such craft should have speeds in the 80-160 knot range and be capable of lifting 500 tons or more to intermediate support bases, sea based complexes, or advanced tactical support base (ATSB) complexes.

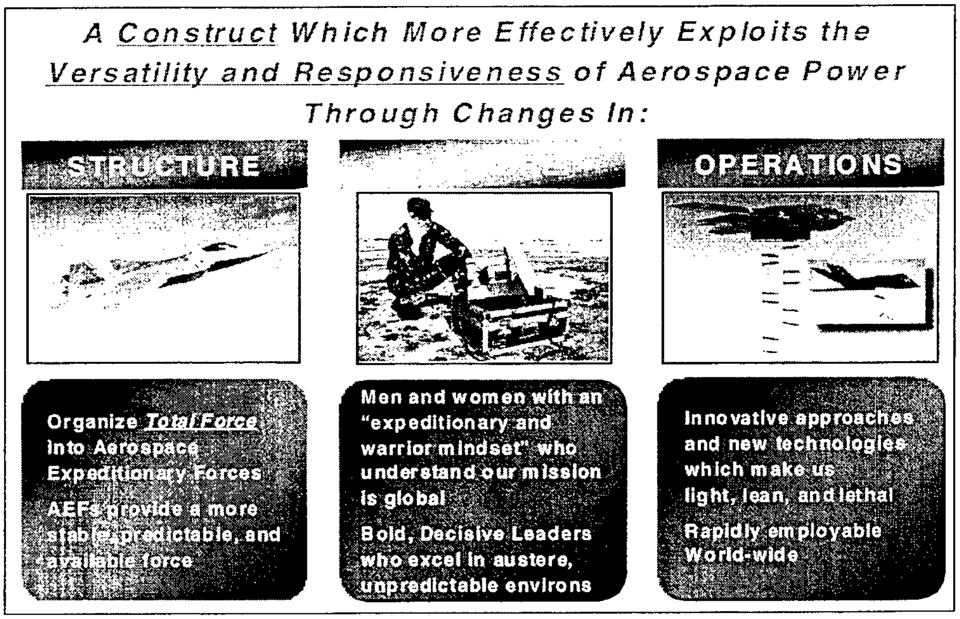


Potential Maritime Solutions

- Military - Develop and acquire sufficient force
- Commercial
    - High Speed Ships with Fast Load and Unload Capability
        - National Defense Features
            - Outsized doors
            - Strengthened Decks, etc.
        - 40+ knots
        - Transit in high sea states
        - Access to ports no less than present
- Air lifter
    - 80-160 knots
    - Lifts 500 tons or more to Intermediate Support Bases and or Sea Base/ATSB Complexes
    - VSTOL/VTOL capability at Sea Basing/ATSB complexes
    - Technical advances may allow novel debarkation
- VTOL on-load/off-load
    - 20 ton lift capability for Sea Base Complexes,combat and austere ports
    - Tactical delivery vice beach depository

Figure 4. Navy Underwriting Joint Vision 2010 and Beyond

Sea-basing and ATSB complexes create a requirement for vertical short take-off and landing (VSTOL) and vertical take-off and landing (VTOL) aircraft. These aircraft would "go both ways." This means a capability of flying long ranges to intermediate support bases and bringing troops and equipment to sea base or ATSB complexes, as well as flying troops and supplies forward to combat areas (operational mobility). Technical advances may allow for novel debarkation methods, such as ship load/unload at austere ports. The requirement for long range VSTOL drives the solution to include a large number of fixed wing VSTOL aircraft for these tasks. Rotorcraft may be employed at shorter ranges. The fixed wing VSTOL aircraft would be designed to transport fighting vehicles as well as troops, supplies, ordnance, and petroleum, oil, and lubricants (POL). The VTOL on-load/off-load requirement would be a 20-ton lift capability for sea base complexes, combat, and austere ports. These aircraft would engage in tactical delivery vice beach and shore base depository.



A Construct Which More Effectively Exploits the Versatility and Responsiveness of Aerospace Power Through Changes In:

STRUCTURE

OPERATIONS

Organize *Total Force* into Aerospace Expeditionary Forces

AEFs provide a more stable, predictable, and available force

Men and women with an "expeditionary and warrior mindset" who understand our mission is global

Bold, Decisive Leaders who excel in austere, unpredictable environs

Innovative approaches and new technologies which make us light, lean, and lethal

Rapidly employable World-wide

Figure 5. Expeditionary Aerospace Force – Our Vision

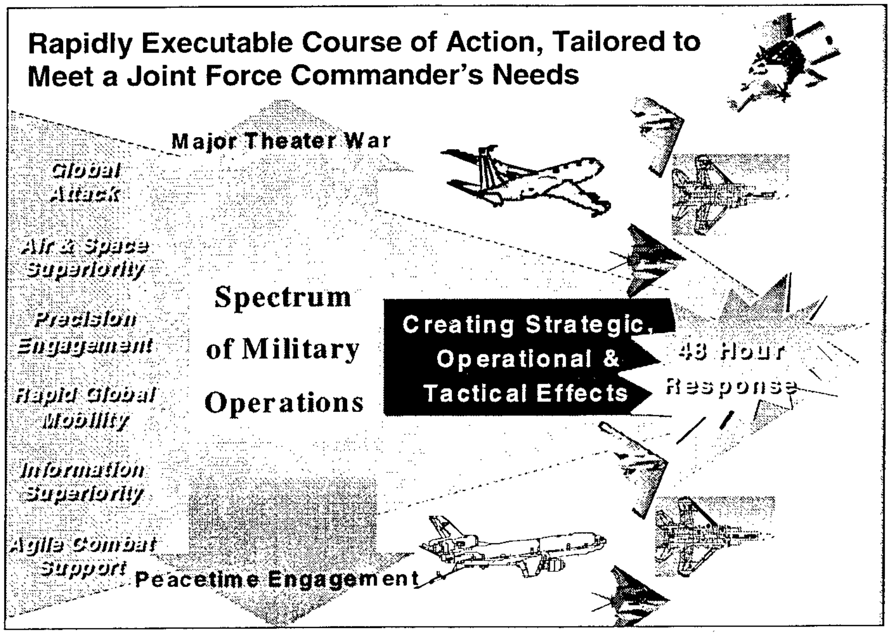
AIR FORCE

The evolution of the total force toward the Air Expeditionary Force (AEF) will involve significant changes at all levels of the U.S. Air Force as well as some changes in joint interfaces. These changes have been categorized into three key areas called vectors – structural, cultural, and operational.

Structural changes involve establishing expeditionary organizations. The AEF vision requires structural changes to enable more responsive force packaging; to provide better visibility into force TEMPO and better detection when the force is stressed; and to focus relief on stressed areas.

Cultural changes involve educating, training, and managing people. Over the past nine years, most airmen have come to understand that recurring expeditionary rotations and contingencies are part of normal, daily Air Force operations. But the processes used to grow and manage these expeditionary airmen in many cases have not evolved to meet this reality.

Operational change encompasses innovative approaches and new technologies that make the force light, lean, lethal, and rapidly deployable and employable worldwide.



Rapidly Executable Course of Action, Tailored to Meet a Joint Force Commander's Needs

Major Theater War

Global Attack

Air & Space Superiority

Precision Engagement

Rapid Global Mobility

Information Superiority

Agile Combat Support

Spectrum of Military Operations

Creating Strategic, Operational & Tactical Effects

48 Hour Response

Peacetime Engagement

Figure 6. Air Expeditionary Force Operations – Original

Operationally and culturally the Air Force vision involves:

- Using aerospace strengths in the form of core competencies
- Across the entire spectrum of military operations

- Creating exactly the right kind of effects and doing so within 48 hours of the order to execute (does not include 24 hours of advance notification)

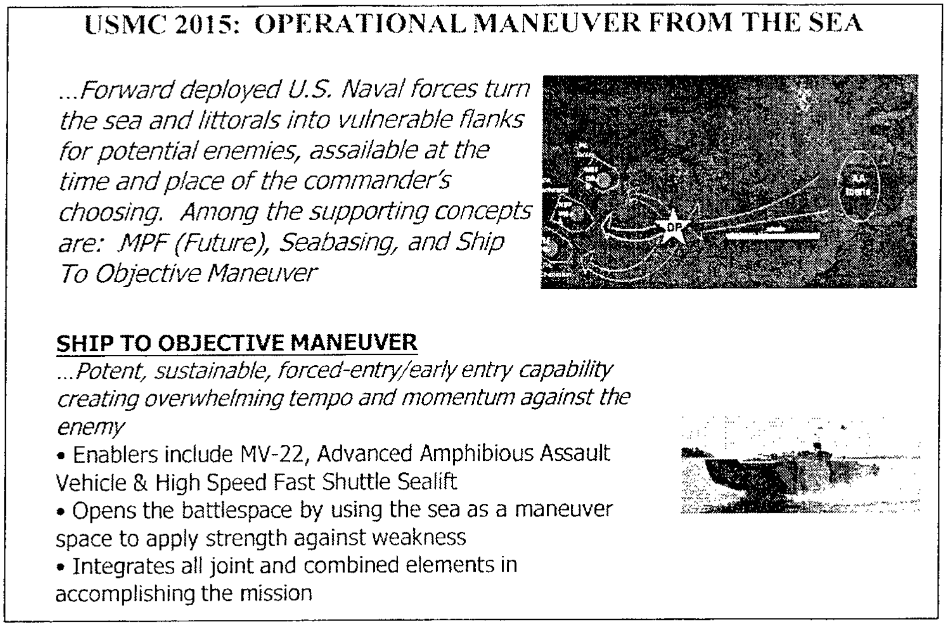
Timing is important

- The demonstrated ability to reach and respond quickly is a deterrent even if forces are not physically present (shaping the environment).
- Quick response can often short-circuit a crisis or at least contain it until more substantive forces can respond (respond).
- This capability also reduces demand for forward presence which allows more forces to be kept home which in turn allows better force sustainment (preparing).

MARINE CORPS

Operational Maneuver From the Sea is the capstone concept that will take DoD's naval forces into the 21st century. Forward deployed U.S. naval forces turn the sea and littorals into vulnerable flanks for potential enemies, assailable at the time and place of the commander's choosing. This capstone concept is supported by a number of concepts such as ship to objective maneuver, maritime pre-positioning force future (MPF-Future), and seabasing.

Ship to objective maneuver employs the concepts of maneuver warfare to project a combined arms force by air and surface against inland objectives with no operational pause on a beachhead or other intermediate assembly point. The enablers for this concept include: MV-22, Advanced Amphibious Assault Vehicle, and High-Speed Fast Shuttle Sealift. In combining all joint and combined elements to accomplish the mission, this potent, sustainable, forced-entry and early-entry capability creates overwhelming tempo and momentum against the enemy. It also requires the enemy to defend a vast area against seaborne mobility and deep power projection. In the end game, the dilemmas imposed upon the enemy by the flexibility of U.S. naval forces will render most of the enemy force irrelevant.



USMC 2015: OPERATIONAL MANEUVER FROM THE SEA

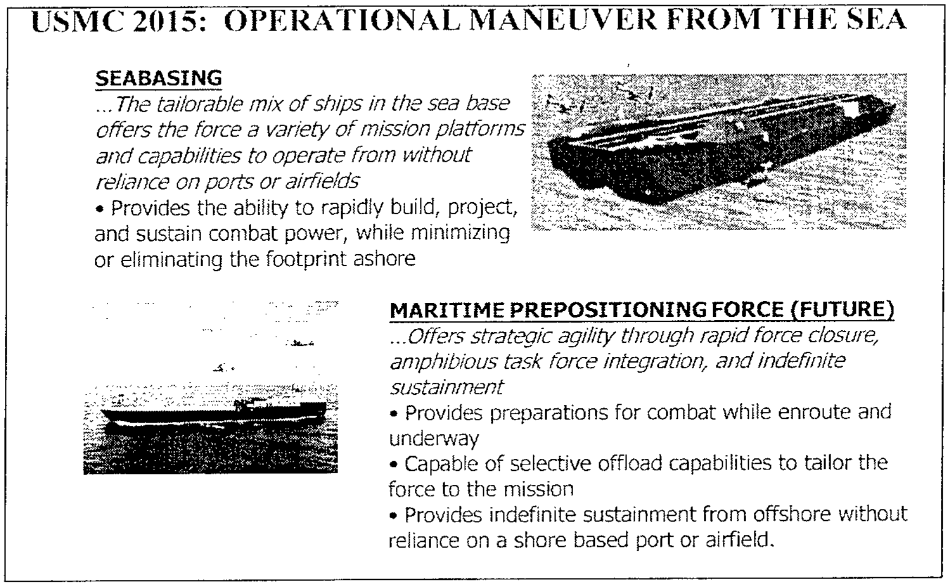
...Forward deployed U.S. Naval forces turn the sea and littorals into vulnerable flanks for potential enemies, assailable at the time and place of the commander's choosing. Among the supporting concepts are: MPF (Future), Seabasing, and Ship To Objective Maneuver

SHIP TO OBJECTIVE MANEUVER

...Potent, sustainable, forced-entry/early entry capability creating overwhelming tempo and momentum against the enemy

- Enablers include MV-22, Advanced Amphibious Assault Vehicle & High Speed Fast Shuttle Sealift
- Opens the battlespace by using the sea as a maneuver space to apply strength against weakness
- Integrates all joint and combined elements in accomplishing the mission

Figure 7. Marine Corps – Ship to Objective Maneuver



USMC 2015: OPERATIONAL MANEUVER FROM THE SEA

SEABASING

...The tailorable mix of ships in the sea base offers the force a variety of mission platforms and capabilities to operate from without reliance on ports or airfields

- Provides the ability to rapidly build, project, and sustain combat power, while minimizing or eliminating the footprint ashore

MARITIME PREPOSITIONING FORCE (FUTURE)

...Offers strategic agility through rapid force closure, amphibious task force integration, and indefinite sustainment

- Provides preparations for combat while enroute and underway
- Capable of selective offload capabilities to tailor the force to the mission
- Provides indefinite sustainment from offshore without reliance on a shore based port or airfield.

Figure 8. Marine Corps Sea-basing and MPF

MPF-Future offers strategic agility through rapid force closure, amphibious task force integration, indefinite sustainment, and reconstitution and redeployment. Force closure will provide for at-sea arrival and assembly of the maritime pre-positioning force (MPF), eliminating the requirement for access to secure ports and airfields. Marines will deploy to meet maritime pre-positioning platforms while they are underway and enroute to objectives. Units will be billeted while completing the process of making their equipment combat ready. Platform design will facilitate this preparation process by easy access to all equipment for inspection, maintenance, testing, and selective reconfiguration of tactical loads. This enhanced force closure characteristic will permit elements of the MPF MAGTF to arrive in the objective area already prepared for operations.

Amphibious task force (ATF) integration will participate in Operational Maneuver From the Sea by using selective offload capabilities to reinforce the assault echelon of an ATF. Maritime pre-positioning ships will be multipurpose in nature and will provide advanced facilities for tactical employment of assault support aircraft, surface assault craft, advanced amphibious assault vehicles, and ships' organic lighterage under conditions of at least sea state three. Furthermore ship communications systems will be fully compatible with the tactical command and control architecture of the ATF.

Indefinite sustainment will be provided by Maritime Pre-positioning Ships serving as a sea-based conduit for logistics support. This support will flow from the United States or overseas, via the sea base, to Marine units conducting operations ashore. Reconstitution and redeployment of Maritime Pre-positioning Ships will be conducted in-theater without a requirement for extensive materiel maintenance or replenishment at a strategic sustainment base. This ability to rapidly reconstitute the MPF MAGTF will allow immediate employment in follow-on missions.

Seabasing allows the force to operate from over the horizon without relying on ports or airfields. The seabase provides the ability to rapidly build, project, and sustain combat power, while minimizing or eliminating the footprint ashore.

Emerging technologies will enable a number of capabilities which will enhance the ability of U.S. forces to project power. Among these technologies are a new class of MPF ships, development of high speed shuttle sealift and lighterage, a new class of light weight fast attack vehicles, improved mine counter-warfare technology, and more lethal long-range precision fires.

DEPLOYMENT AND SUSTAINMENT

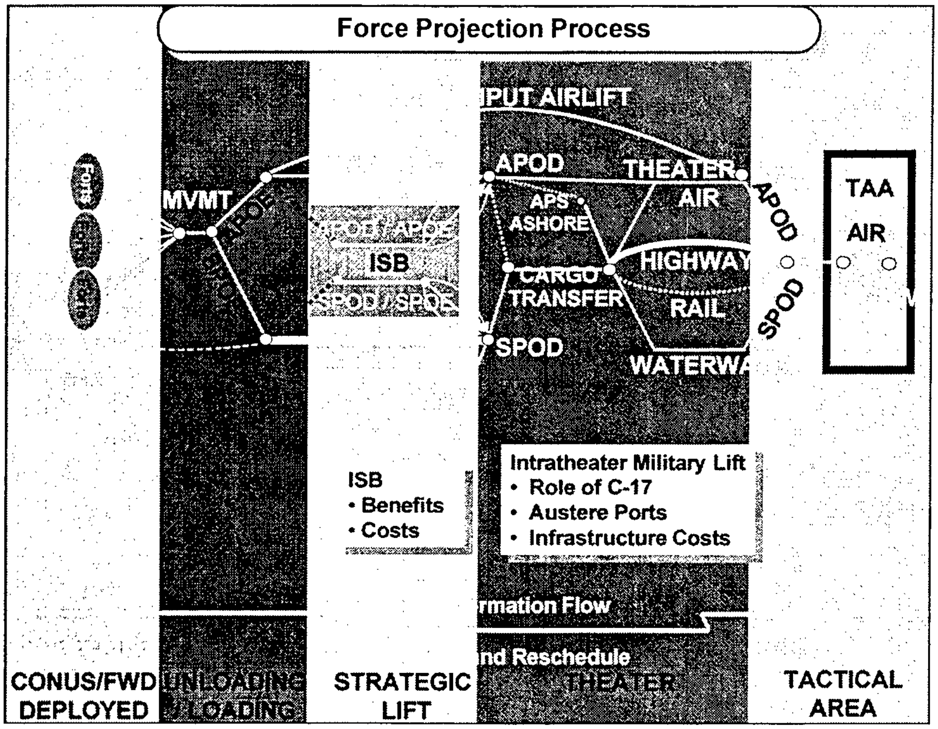


Figure 9. Force Protection Process

Today's deployment process is slow and vulnerable. To reduce deployment time, DoD needs to consider the entire throughput process, which involves the following:

- ***Deployment tools.*** Commanders do not have good automated movement planning tools. Scheduling, monitoring, and rescheduling tools are not timely. Moreover, the deployment process has major nodal vulnerabilities.

- ***Deployment requirements.*** Reducing logistics consumption reduces deployment requirements. Split basing can increase combat power availability and may require organizational redesign.

- ***Early Entry Forces.*** Lighter, lethal, and efficient forces are needed. Current joint forces and their logistics are heavy and bulky and are neither designed nor packaged for extensive use of commercial air freight. DoD organic airlift is not projected to grow significantly.

- ***Follow-on Forces.*** Once ships begin arriving, their capacity outpaces air capacity. Except for current early entry Army airborne and Marine units, all Services are air base and/or port dependent with DoD or commercial ships.

- ***Commercial Capabilties.*** Commercial lift and overall throughput capacity outpaces military lift capability but economic and technical changes are limiting their availability. DoD mechanisms to employ commercial capabilities are becoming ineffective.
- ***Vulnerable Nodal Process.*** The current DoD deployment sustainment process is traditionally nodal and heavily, but not totally, dependent on high quality, air and sea ports, and also on reception, staging, and onward integration (RSOI), the exceptions are deliveries to well-protected or out-of-threat reach air bases and the insertion of Marine and Army intervention forces.

Commercial Trends

Commercial trends in freight and information technology will have a significant impact on the deployment sustainment system. Most significant among these developments are:

- ***National Land Freight.*** Consolidation and economics producing a sparse transcontinental rail "super highway" will likely result in decreased military unit and logistics rail access and longer fort-to-port deliver times.
- ***Worldwide Air Freight.*** Today air freight capacity is about 50 kt/day throughput and is projected to grow to 200 kt/day by 2025 (DoD is approximately 8 kt/day). Substantial conversions (up to 600 in the next 15 years) will create the opportunity for DoD to use the original civil air reserve fleet (CRAF) concept and have installed defense features.
- ***Worldwide Sea Freight.*** Fewer large [(6,000-8,000 twenty-foot equivalent unit (TEU)] container ships, using small numbers of very high capacity deep-water ports and fewer routes. Currently, there are one thousand plus, TEU ships (largely foreign flag) available. Military useful commercial roll-on, roll-off (RORO) fleet (231) and U.S. military fleet (57) is static at best. Fast load/unload and transit ships offer great advantages to the DoD and are becoming available.
- ***Information Technology & Logistics.*** Revolutionary changes have already taken place in integrated use of tagging, tracking, and optimization of throughput using real time information technology systems. DoD is well behind the commercial practices and needs to catch up quickly.
  - Information technology is integrated and optimized in the commercial enterprise
  - DoD does fragmented integration
  - Commercial industry containerizes, which minimizes handling touches and time
  - Much of DoD material handling is breakbulk requiring more touches and time

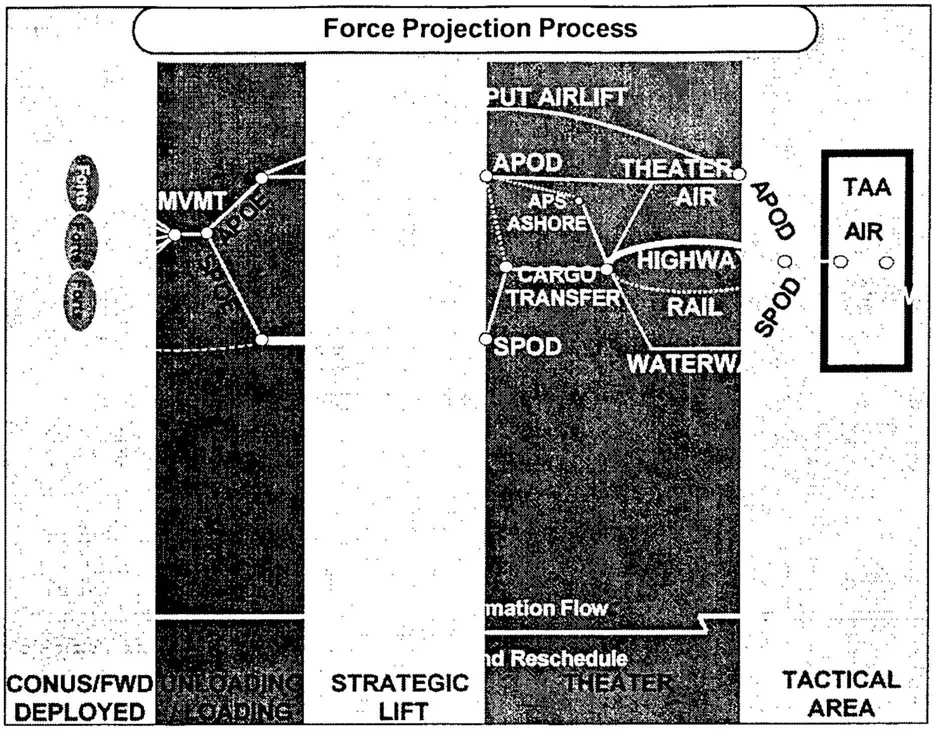
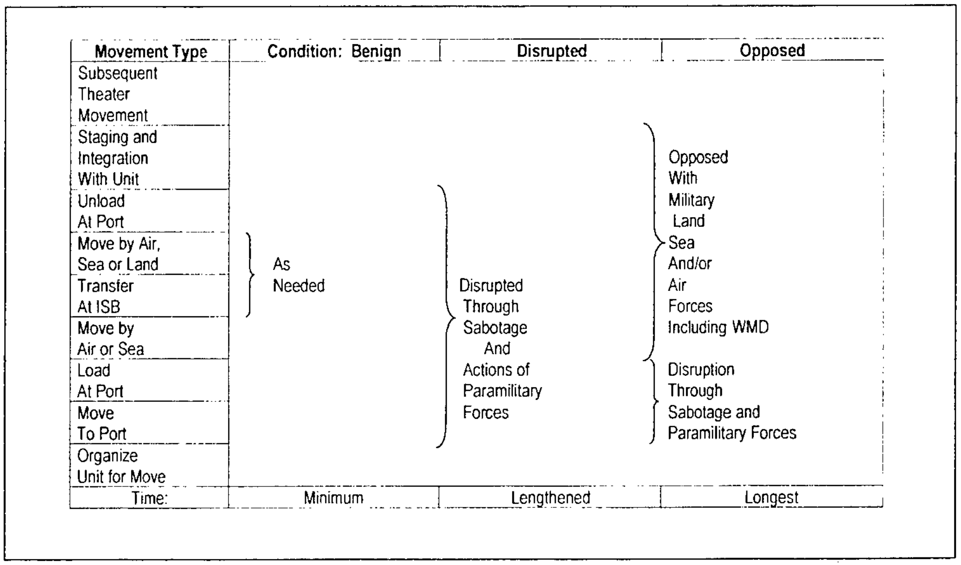


Figure 10. Force Protection Process

A thinking enemy could engage and disrupt the joint force deployment. Figure 11 depicts notional actions directed against the stages of the deployment-sustainment process.



Movement Type	Condition: Benign	Disrupted	Opposed
Subsequent Theater Movement			
Staging and Integration With Unit			Opposed With Military Land Sea And/or Air Forces Including WMD
Unload At Port		Disrupted Through Sabotage And Actions of Paramilitary Forces	
Move by Air, Sea or Land	As Needed		
Transfer At ISB			
Move by Air or Sea			
Load At Port			Disruption Through Sabotage and Paramilitary Forces
Move To Port			
Organize Unit for Move			
Time:	Minimum	Lengthened	Longest

Figure 11. Opportunities for a Thinking Enemy

AN IMPROVED PROCESS

Early entry land, sea, and air forces are intended to deter, deny enemy set, secure bases, and be part of later actions with follow-on forces to achieve campaign objectives. To have greater strategic agility, these forces must adopt the capabilities described in Figure 12 below.

Leverage commercial capabilities which are part of the solution for benign, disrupted, and opposed entry cases.

- Focus on gaining assured access to area of operation by two mechanisms when opposed or disrupted
  - Develop capabilities to employ austere and unpredictable air and sea force insertion points as contrasted with known ports of entry for early entry intervention forces
  - Eliminate the need for RSOI process for forces and supplies. Insertion points should be transient and distributed
- Sustainment needs to be distributed (pipeline) based, not nodally based
- Seize and protect airports, bases, and seaports as necessary
- Employ forces capable of distant fires (as appropriate)

Figure 12. A Possible Approach to Strategic Agility for Early Entry Forces

Army and Marine forces are intended to be capable of assured early theater access in substantial numbers by air and/or sea using austere, unpredictable, and transiently occupied entry points. These forces should also be ready to fight on insertion (no RSOI) and employed in large but distributed formation (brigades, battalions), constituted with network centric teams having organic weapons and C^4ISR along with higher echelon and joint capabilities. These forces should be endowed with great lethality, mobility, and multi-faceted survivability and configured to mass effects through use of own and joint fires, mobility and sustainment. The forces should be sustainable for a period of time with both organic resources and non-nodal joint logistics capabilities that do not require interior protected lines. Finally, operationally and technologically, the force should enhance follow-on traditional legacy forces and systems.

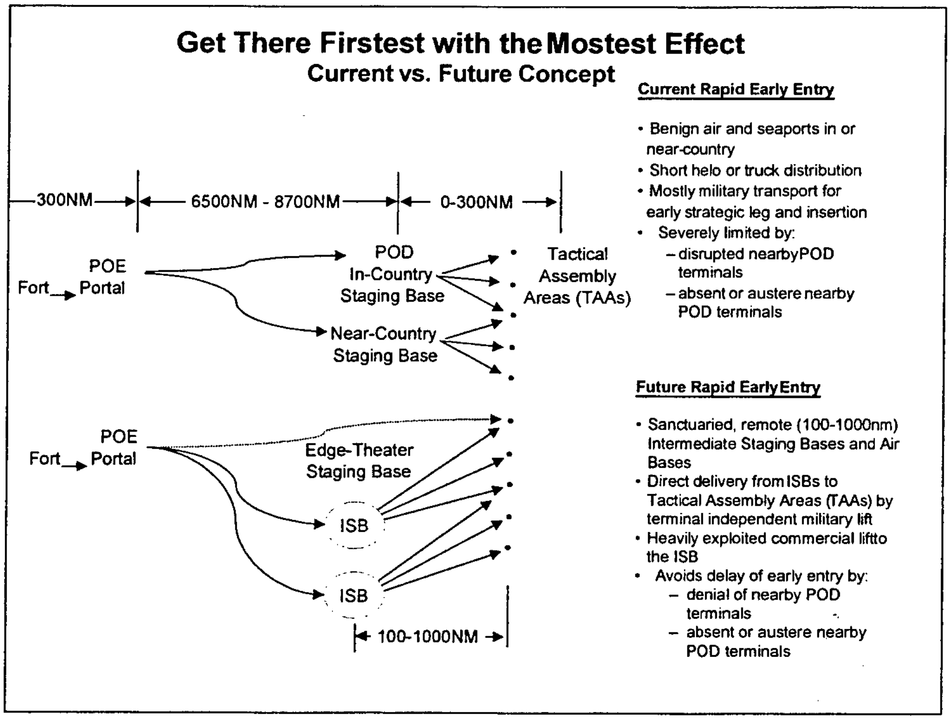
Theater air forces include theater or near-theater land-based, sea-based, other forward-based, and CONUS-based airpower. Of these, the theater or near-theater basing and sustainment provide the greatest challenge. Bases and supply systems must either be outside the area of direct enemy attack or be protected against it. Force protection to deal with paramilitary threats must obviously be provided in all cases. To be most efficient, air bases should be employed within 300 nautical miles of areas of employment. Tanker support can extend this substantially but brings with it additional resource needs and adds time to the force deployment process.

The Marines have configured their early entry units to underwrite the suggested process. Their capabilities will include entry by sea and air at unpredictable locations. Their follow-on forces, like most of the Army's, are currently port dependent.

Sustainment of all forces presents a continuing challenge even if early entry land and air forces operate with non-traditional logistic systems which do not require protected interior lines (employing means such as air delivery). Follow-on forces are existing and/or upgraded legacy forces whose platform bulk and large sustainment needs require either fixed ports with substantial protection or a major advance in high speed unloading features at austere and unpredictable ports.

All of the above assume two things: 1) that improvements are made in the accuracy, timeliness, and continuing management of this rather different deployment-sustainment process and 2) that DoD establishes positive partnership arrangements with commercial transportation communities to employ the extensive capabilities of this sector for strategic deployment and the operation of CONUS and intermediate strategic bases (ISB).

Figure 13 is a simplified graphic of the suggested concept. ISBs must be sufficiently numerous, operated like commercial "hubs," and capable of supporting the needed throughput which can be driven with commercial assets and rapidly cycled into austere locations by military air configured for this mission. Neither military nor commercial sealift is configured for high-speed austere port load or unload. Joint logistics over-the-shore (JLOTs) does not satisfy this need for early entry forces.



Get There Firstest with the Mostest Effect
Current vs. Future Concept

Current Rapid Early Entry

- Benign air and seaports in or near-country
- Short helo or truck distribution
- Mostly military transport for early strategic leg and insertion
- Severely limited by:
  - disrupted nearbyPOD terminals
  - absent or austere nearby POD terminals

Future Rapid EarlyEntry

- Sanctuaried, remote (100-1000nm) Intermediate Staging Bases and Air Bases
- Direct delivery from ISBs to Tactical Assembly Areas (TAAs) by terminal independent military lift
- Heavily exploited commercial liftto the ISB
- Avoids delay of early entry by:
  - denial of nearby POD terminals
  - absent or austere nearby POD terminals

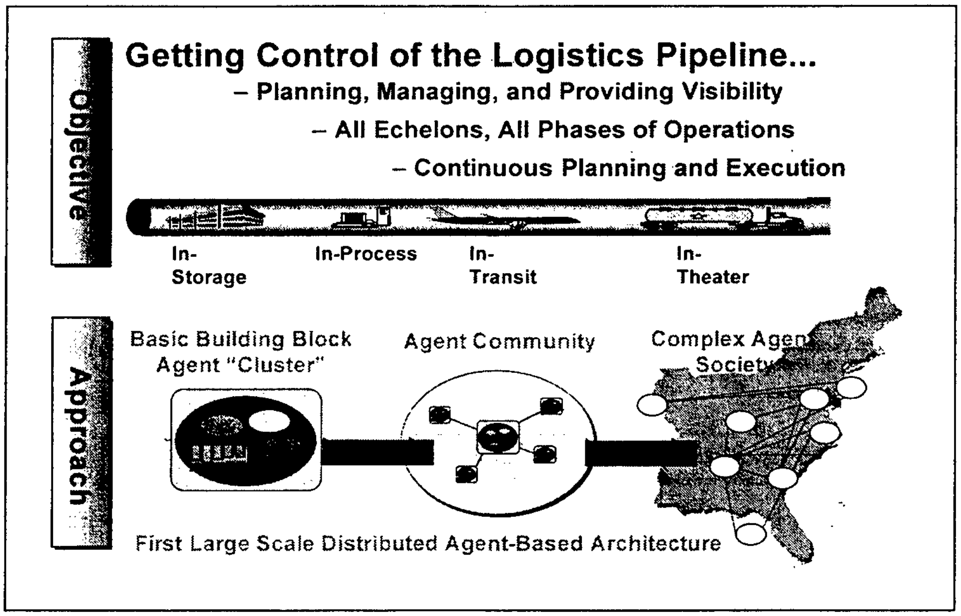
Figure 13. Get There First with the Most Effect (Current vs. Future Concept)

IMPROVING COMMAND CONTROL FOR DEPLOYMENT AND SUSTAINMENT

In order to meet the shorter strategic maneuver timelines needed, significant improvements in command and control (C^2) are necessary to allow planners to:

- Plan deployments faster
- Minimize lift for systems and support with split-based operations
- Re-plan while en route
- Support sustainment with information systems for anticipatory logistic
- Minimize forward sustainment needs with information systems

The Advanced Logistics Project (ALP) architecture could enable a fundamental change in the way DoD does business in logistics, as shown in Figure 14. The ALP is a jointly funded initiative between the Defense Advanced Research Projects Agency (DARPA) and the Defense Logistics Agency (DLA), in partnership with the U.S. Transportation Command (TRANSCOM) and the Joint Staff J-4 Directorate. ALP is focused on developing and demonstrating advanced information technologies that will allow DoD to get control of the logistics pipeline and the entire logistics business process. The project is to define, develop, and demonstrate fundamental enabling technologies to allow logistics and transportation assets to be deployed, tracked, sustained, and redeployed more efficiently than ever before.



Objective

Getting Control of the Logistics Pipeline...

– Planning, Managing, and Providing Visibility

– All Echelons, All Phases of Operations

– Continuous Planning and Execution

Approach

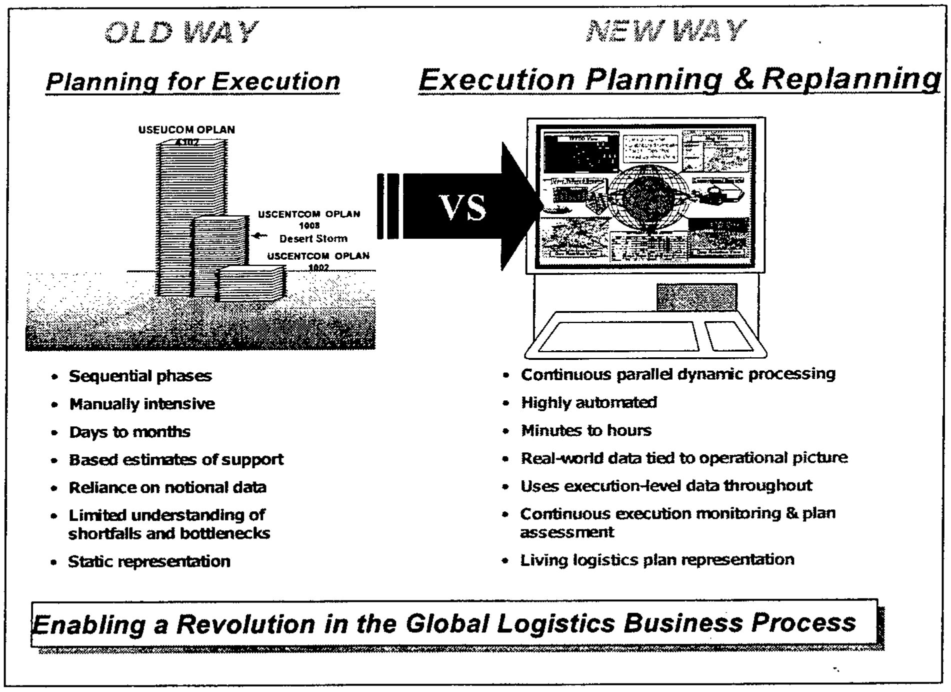
First Large Scale Distributed Agent-Based Architecture

Figure 14. ALP Approach to JV2010 Focused Logistics

The technical approach uses a distributed agent-based architecture. The system's basic building block is the "cluster." Each cluster is made up of a similar set of components and functions in a manner modeled after the human cognitive process. While clusters are structurally similar, they can be specialized to accomplish specific functional behaviors using software plug-ins. For example, a cluster in a truck battalion may schedule truck assets, while a similar cluster with different plug-ins may operate at TRANSCOM headquarters selecting global nodes for the shipment of units and equipment. Individual clusters performing similar and complementary functions can be grouped to form "communities" representing a specific organization. Communities can be grouped to form "societies." In this way the entire logistics business process can be represented.

ALP Operational Vision

ALP's advantages over the segmented DoD improvements lie in its ability to employ both DoD and commercial nodules. It could move the Department from an environment where planning is focused on execution, that is deliberate planning, to an environment where execution, monitoring, and replanning can occur in real time against real information. This approach will require DoD to implement process improvements, which would bring overall logistics performance in line with best commercial practices and resulting performance.



OLD WAY

Planning for Execution

- Sequential phases
- Manually intensive
- Days to months
- Based estimates of support
- Reliance on notional data
- Limited understanding of shortfalls and bottlenecks
- Static representation

NEW WAY

Execution Planning & Replanning

- Continuous parallel dynamic processing
- Highly automated
- Minutes to hours
- Real-world data tied to operational picture
- Uses execution-level data throughout
- Continuous execution monitoring & plan assessment
- Living logistics plan representation

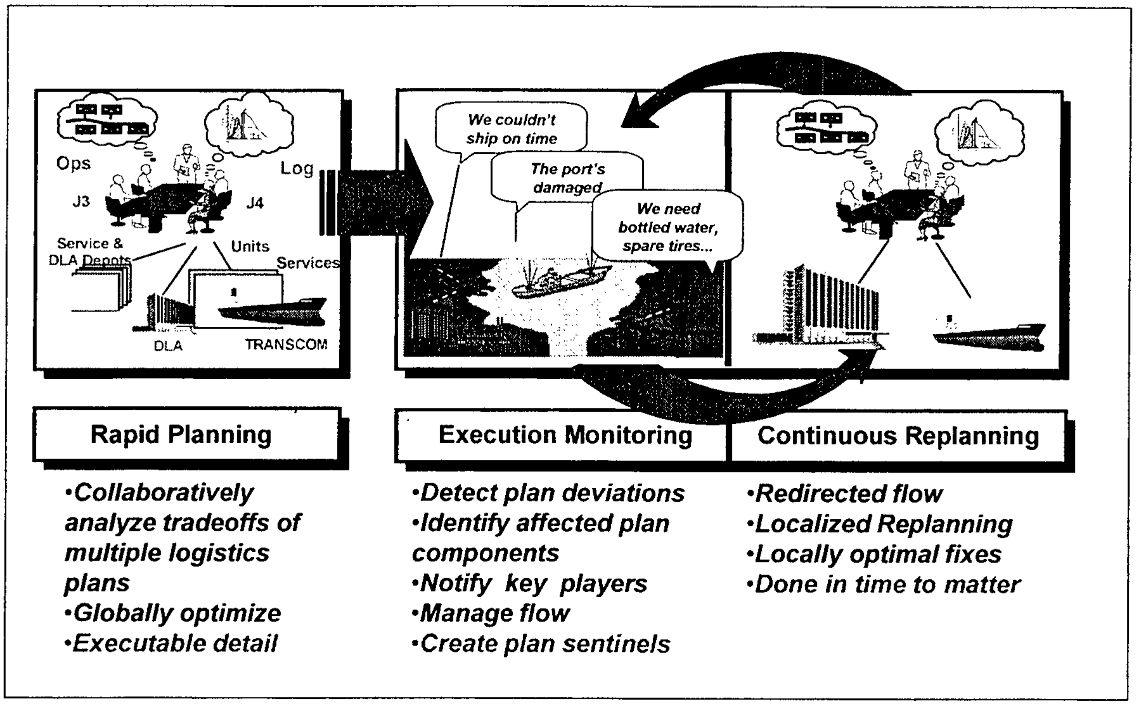
Enabling a Revolution in the Global Logistics Business Process

Figure 15. Advanced Logistics Process

A focused logistics process enabled by ALP involves:

- Continuous parallel dynamic processing vs. sequential phasing
  - Highly automated versus manually intensive
  - Planning time reduced from days/months to minutes/hours
  - Deliberate deployment planning: 1 year +
  - Contingency execution planning: 8-10 days
  - Execution planning time of 72-108 hours, in near-term
  - Continuous execution planning of 1-4 hours

ALP uses real execution-level data rather than relying on notional data. The system provides live, continuous execution monitoring and plan assessment rather than limited projection of expected bottlenecks and shortfalls. ALP provides an environment for living log plan representation instead of static snapshot. Figure 16 illustrates the operational vision enabled by ALP.



Rapid Planning

•Collaboratively analyze tradeoffs of multiple logistics plans
•Globally optimize
•Executable detail

Execution Monitoring

•Detect plan deviations
•Identify affected plan components
•Notify key players
•Manage flow
•Create plan sentinels

Continuous Replanning

•Redirected flow
•Localized Replanning
•Locally optimal fixes
•Done in time to matter

Figure 16. ALP Operational Vision

ALP is building an information technology infrastructure to enable operators and logisticians at any echelon, to work together with the Services, the Defense Agencies and support organizations to quickly develop plans to Level 5 detail based on real, rather than notional data. With this executive level of detail, DoD could transition seamlessly from planning to execution with confidence. Using plan sentinels against real world data feeds, commanders could monitor execution to predict and detect deviations to the plan in a timely manner and automatically begin replanning. The ALP system will automatically do plan repair routines and present recommendations to commanders, which would modify the plan in an optimum fashion to keep the operation on track.

ALP is to be available within two years. When it reaches maturity and is transitioned to operational use, it will revolutionize command and control. Most importantly, ALP's architecture will provide mixing and matching of DoD and commercial capabilities. An example of the kind of mixing and matching possible would be to combine Wal-Mart warehousing and Fed Ex registering and tracking with DoD's Joint Tactical Asset Visibility (JTAV) and global transportation network (GTN) to put together a "best of breed" information technology suite. Currently there is no firm transition plan for ALP, but the Joint Staff and the Army are addressing such possibilities.

IMPROVING EARLY ENTRY BY AIR

All the Services – Army, Navy, Marines and Air Force units – which require airlift for rapid power projection have heavy and bulky equipment (unit weights of thousands to ten thousands of tons) and have substantial resupply requirements (thousands of tons per day). The Army's 70 ton tanks (used also by the Marines) are the "bumper sticker" example of the heavy force but the facts are otherwise.

TRANSCOM's future strategic fleet structure could be 246 aircraft including 120 C-17s. Cargo throughput capability is approximately 50 million-ton-miles per day, including the Civil Reserve Air Fleet. It is important to note today that CRAF represents a substantial portion of the required strategic airlift capability but it is employed almost totally to move people.

In the future, CRAF could be the dominant strategic lift component, providing the DoD with a non-organic air lift fleet of traditional and non-traditional CRAF platforms. This will save DoD the expense of expanding its strategic lift fleet and allows the C-17 to be freed for intra-theater lift to augment the C-130 fleet. This approach dramatically expands theater capabilities because of the 60-ton C-17 payload and its shorter landing and takeoff requirements.

It is worth noting that TRANSCOM's future planning show no growth in CRAF capabilities, yet projections by several sources show commercial fleet growth rates of 7 percent per year. Exploring this disconnect suggests that TRANSCOM has received no requirement for additional CRAF support. As previously shown, the DoD air throughput capacity is 15 percent of daily commercial capacity. In 2020, it will probably be 5 percent or less. For DoD to leverage the large and growing fleet it must address both technical and business challenges. Leveraging will require collaboration, adaptation, and selective stimulation.

TECHNICAL AND BUSINESS CHALLENGES

There are a number of technical challenges that must be addressed in order to employ commercial assets for air lift. These include limitations on door sizes, floor strengths, rapid loading and unloading, and handling equipment. In addition, the current CRAF policy and implementation would have to be improved. Innovations such as the Virtual Airlines Program at DARPA should be exploited and expanded to extend from the passenger domain, to the freight domain, and then further to sea and U.S. railroad usage. The "virtual airline" concept holds the promise of a win-win partnership between DoD and the commercial transportation sector. Simulation testing using Gulf War demands and an adaptation of the FAA collaborative decision-making methodology showed how successful "virtual airline" could be.

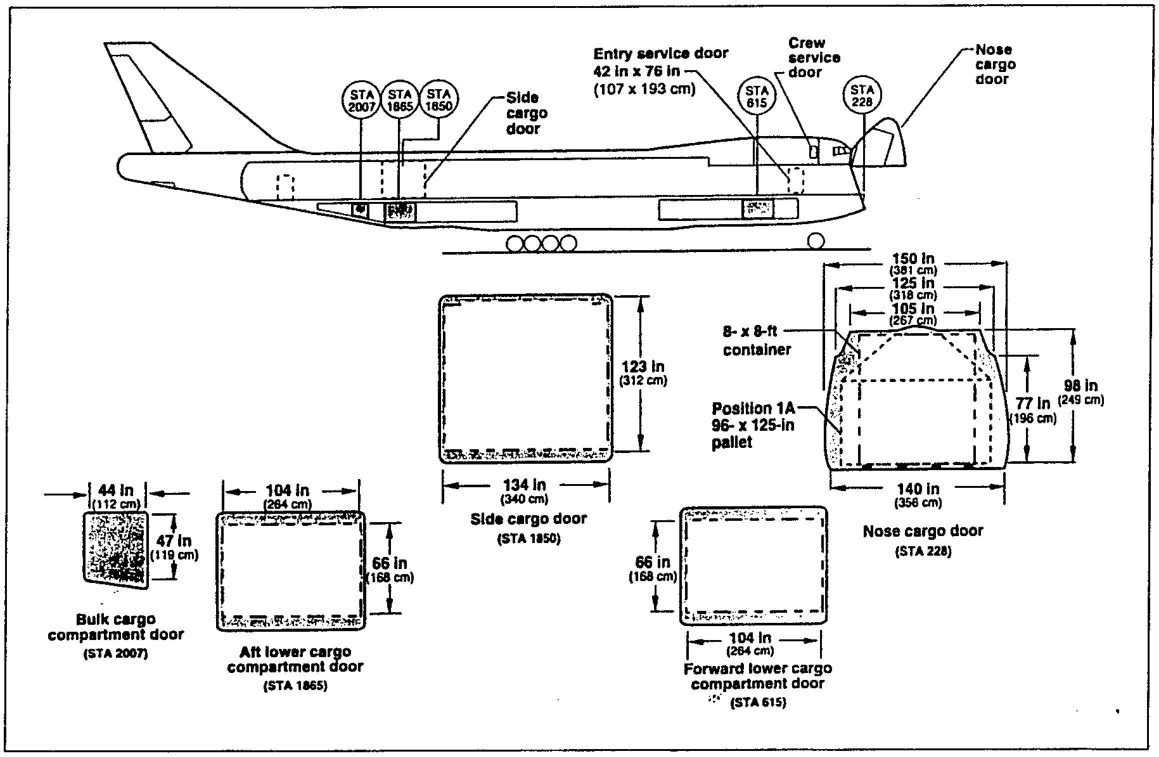


Figure 17. Door and Floor Constraints

The Military Traffic Management Command Transportation Engineering Agency (MTMC-TEA) should evaluate commercial airlift compatibility with current early entry equipment and explore high-payoff, military-specific enhancements to the commercial fleet. Since many air freighters are grown from converted passenger aircraft, TRANSCOM and the Services should take advantage of this opportunity to obtain features for DoD use. TRANSCOM and the Services should jointly sponsor expansion of the “Virtual Airline” work conducted by DARPA.

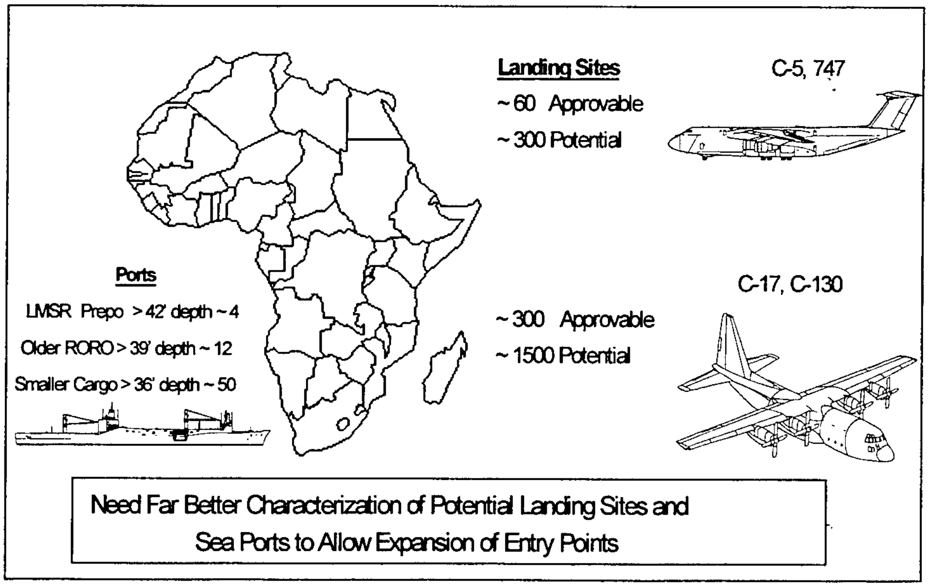
Weight, size, and density affect loading. As an example the entire air lift fleet (commercial, military fixed wing, and military rotary wing) can be employed for both rapid strategic and operational/tactical movement for vehicle weights of nine tons or less (with volumes less than 20’x8’x8’). For loads greater than nine tons, the CH-47 fleet is not usable and at 14 tons the CH-53 is not usable. Beyond 20 tons, the C-130 is not usable. Commercial airfreight requires no special support at 9 tons. But for vehicle weights of 20 tons, commercial air likely requires cribbing and the corresponding increased loading and unloading times. Beyond 20 tons, the C-5 and C-17 fleet must provide all the lift. Losing the vertical take-off and landing capability reduces access by an order-of-magnitude. Losing the C-130 and commercial fleets reduces capacity by at least 80,000 tons leaving only 15,000 tons of military lift to do the entire task of moving a joint force in excess of 100,000 to 200,000 tons.

In the mid- to far-term, 2015 to 2025, DoD might acquire a super short take-of and landing (SSTOL) for operational lift (replace the C-130) and improved VTOL/JTR capability to replace the CH-47 and CH-53. In this case, the 9-ton break point might shift to 12 tons. The C-130 break point could move up to 30 tons but the impact on commercial lift is the same in terms of vehicle tonnage, and the lift fleet potential is estimated at 200,000 tons. That is a large "give up."

The Army, on behalf of DoD, should undertake an initiative with its MTMC-TEA to find the limits of techniques to accommodate future and selected current vehicles at the least time penalty. This agency, which is an engineering activity, should determine how heavier vehicles might be accommodated (possibly up to 15 or even 20 tons) and how the loading of these might be rapid and efficient.

Freedom of Access – Operational and Tactical Air Mobility

Early entry forces must be deployed rapidly enough to prevent the enemy from setting the conditions of the battlespace or, more ideally, from even escalating to a significant level of belligerency. To accomplish this, necessary lift, timely generation of forces, and access are required. Figure 18 shows that airfield access would seem large enough (though not necessarily strong enough) for particular aircraft in Africa, as well as seaports. The C-5 and 747 can access approximately the same number of potential airfield sites, with the 747 accessing slightly more (based on runway dimensions). The C-17 and C-130, with shorter runway needs, have potential access to many more airfields. For seaports, only a few ports are large medium-speed roll-on/roll-off (LMSR) capable.



Need Far Better Characterization of Potential Landing Sites and Sea Ports to Allow Expansion of Entry Points

Figure 18. Limitations on Access

Unfortunately, only one fifth of the large airfields (>6,000 feet long, paved runways) are reliably known to possess adequate bearing strength for large aircraft. Fewer than one tenth of the smaller airfields (>3,000 feet long both paved and unpaved) can be used for landing (even though the C-17 and C-130 possess soft field landing gear) because of poor data on field surface bearing strength. Without better airfield characterization, heavy cargo aircraft are likely to be precluded from supporting early entry through closely proximate in-theater staging bases. Intra-theater aircraft will likely be limited to a few proximate fields which can be easily targeted by a thinking enemy even with limited resources for airfield disruption. Since many of the ports and airfields are built using funding provided by the United States and its allies, such facilities should be tailored to meet DoD needs as part of the requirements.

Consequently, the concept to underwrite strategic maneuver involves, in its more extreme cases, the need to bring equipment and men by commercial and military air and sea into intermediate staging bases, somewhat remote from the tactical assembly areas, and insert them from the ISBs into the militarily active areas of theater by means such as C-17s and C-130s (and the C-130 replacement). There is great benefit to this approach, particularly if airfield surveys validate landing at a higher percentage of the known 3,000 foot strips. This denies the thinking enemy some foreknowledge of insertion points. On the other hand, delivery into a limited set of known locations provides the enemy with an opportunity to interdict these known insertion points by disruption or direct attack.

In addition to increased access to surveyed airfields, the C-17 and the C-130 could use road segments and appropriate open fields, provided these were adequately surveyed and assured ahead of time. Concepts such as the Super Short Take-off and Landing make this even more viable. Further, advanced rotorcraft concepts for heavier loads and much longer ranges might allow truly flexible force insertion. Similarly, tilt rotors and traditional and non-traditional rotary wing aircraft might be developed and acquired to perform this mission, provided they become affordable and sufficiently efficient. A hybrid airship might be employed in a vertical take-off and landing mode under conditions in which its fuel load is appropriate, assuming, of course, that these airships are developed and employed in commercial applications and therefore available.

One of the complexities associated with this choice is the fact that current military fixed wing aircraft are four times more efficient than current helicopters in terms of fuel usage, and their ranges are ten times greater. Further, their cost per pound of empty weight is substantially less. Since insertion in the theater should be done under conditions where the aircraft do not have to be refueled or maintained at the insertion point, fixed wing aircraft have an advantage in this regard because of their overall flight efficiencies and long operating radii.

Access is portrayed, in Figure 19, for the variety of aircraft that are being considered. When the required runway bearing strength and apron area are available, the C-130 and C-17 enjoy at least a half an order-of-magnitude advantage over the C-5 and 747. SSTOL enjoys a potential advantage beyond that.

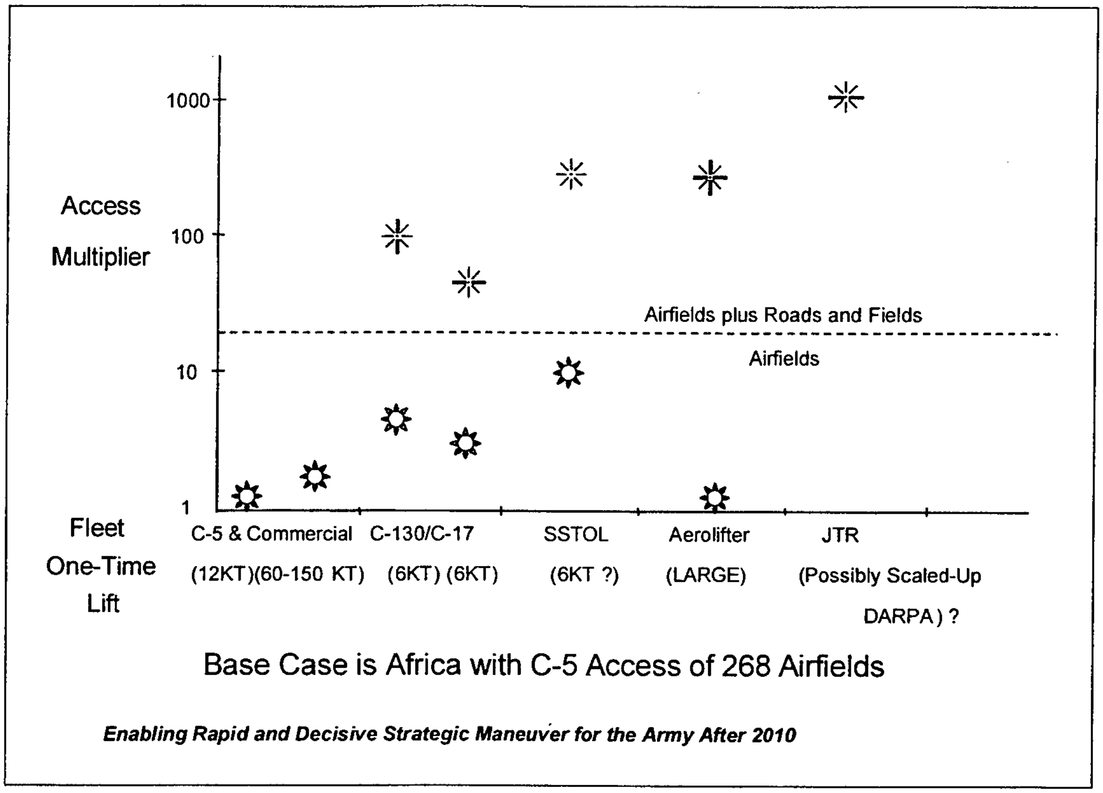


Figure 19. Freedom of Access – Air Mobility (Operational/Tactical)

A major change occurs when roads and open fields are added to the possible inventory of landing sites. C-130s and C-17s enjoy an order-of-magnitude improvement. The SSTOL adds an order-of-magnitude beyond its already existing advantage. Vertical takeoff and landing capabilities expand potential landing sites further (they also require much simpler site surveys). Additional airfield survey and road or field use provide access improvements by 2.5-3 orders-of-magnitude beyond that available with the C-5 alone.

In viewing the trends, it is clear that the first big access improvement occurs when using C-130 and C-17 austere landing capabilities that exist today. As technology opens the possibility for SSTOL, it clearly becomes an advantageous choice, with an accessibility factor of three or more than the C-17 and the C-130. The Army, Air Force, and Marines should work closely with the development activities for the SSTOL. Similarly, a joint tilt rotor or a scaled up version of the current DARPA unmanned endurance helicopter program might provide a VTOL solution, although substantial technology advances are required to improve range, fuel efficiency, and cost. A full spectrum joint warfighting capabilities assessment will be needed to develop priorities for technologies which best support early entry.

EARLY ENTRY BY AIR – FINDINGS

The material reviewed so far suggest the following:

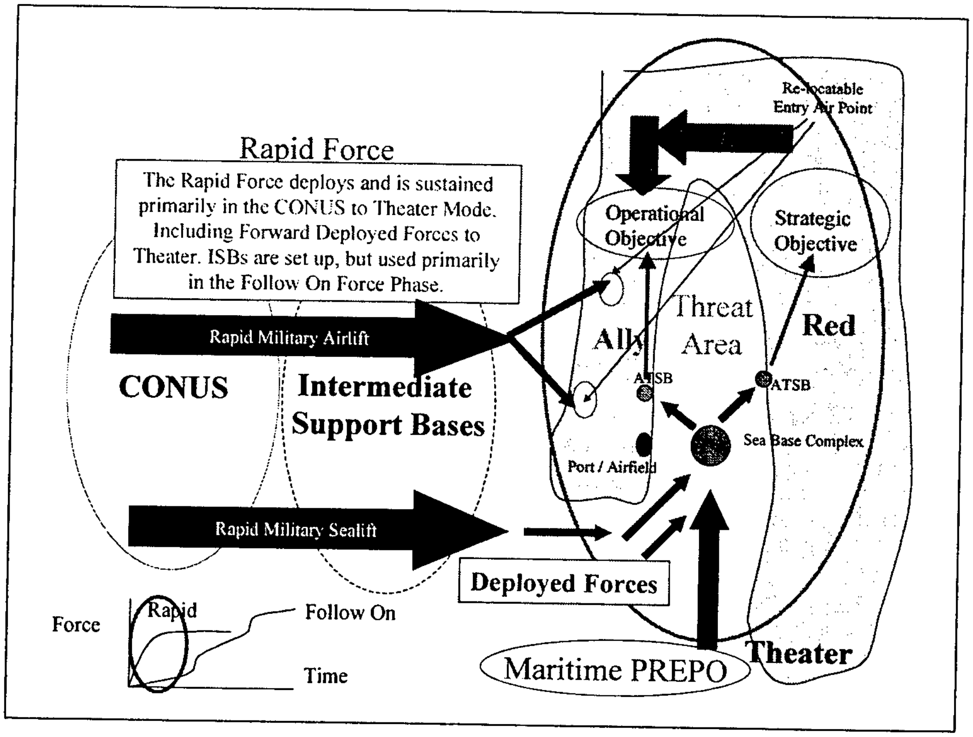
- DoD should make commercial adaptation and stimulation a first line activity because of the benefits that it would create for strategic maneuver.
- The most cost-effective support is derived from adapting and stimulating commercial air lift, both traditional and non-traditional. The "virtual airline" program should be expanded to freight for air, sea, and land movement.
- C-17 and C-130 capabilities should be exploited for the early entry force as an initial effort, with a follow-on focus on greater airfield-independent SSTOL or VTOL.
- Weight and cube of future vehicles and equipment should be adapted to the limits imposed by commercial assets (9 tons in less than 8 x 8 x 20 feet) or develop floor appliqués to allow for 18 to 20 tons in the same volume.
- Develop databases and intellectual infrastructure to optimize the selection and use of distributed intermediate staging bases and theater access points.
- Leverage U.S., but non-DoD, investments such as those from the World Bank and the International Monetary Fund to make entry point infrastructure usable by DoD.
- Make intermodal swiftness a critical vehicle and cargo design parameter.

IMPROVING EARLY ENTRY FROM THE SEA

This chapter deals with rapid assured access from the sea. Three exemplary cases are treated. The first is an expansion of the Marine Operational Maneuver from the Sea capability and would require a DoD only acquisition program. The second exploits commercial possibilities, and the third is a time saving "CONUS PREPO" method.

EXPANSION OF OPERATIONAL MANEUVER FROM THE SEA CAPABILITIES

Figure 20 shows the sequence of the concept of rapid deployment operations. The first step is to set up the intermediate support bases, which must become a continuing part of deployment planning. Once C-Day is declared (presumably in a timely manner based on superior intelligence) and forces start deploying, naval and air combatant units must achieve acceptable levels of air, sea, and littoral supremacy. Initial attacks will be from long-range bombers and tactical land- and sea-based aircraft and missiles.



Rapid Force

The Rapid Force deploys and is sustained primarily in the CONUS to Theater Mode. Including Forward Deployed Forces to Theater. ISBs are set up, but used primarily in the Follow On Force Phase.

Figure 21. Joint Concept for Strategic and Operational Agility Distributed Agile Deployment and Sustainment (DADS)

The next step is to rapidly establish the initial rapid deployment air and sea bridges to the theater. Then the sea-basing complex will start to build. Initial force insertions would take place using deployed amphibious forces and CONUS-to-combat air insertions. These air insertions would go into unpredictable land entry points in minimum threat areas on acceptable rough terrain. Then insertion of forces from sea bases and further amphibious forces would take place.

Maritime pre-positioned material would begin to arrive and marry-up with forces at unpredictable points (sea bases and land entry points). Ground force employment would begin, originating from land entry points (air insertion), sea-base complexes (SBC), and amphibious forces. Amphibious forces would seize areas along the littoral for advanced tactical support bases as required. Sea-base complexes would be logistic and force employment hubs for one or more ATSB. Forces would be sustained through unpredictable logistic points (land movable logistic points) and through sea bases and intra-theater lift.

This operational approach suggests several opportunities:

- Develop operational requirements for unpredictable force entry and sustainment points, including re-locatable entry air points (REAP), sea-basing complexes and advanced tactical support bases.

- Develop plans for intermediate support bases associated with each current and emerging potential crisis theater.

Figure 21 shows the result of a naval maneuver to set up a sea-base complex and an advanced tactical support base. A sea-base complex may act as the "hub" for several ATSBs along the littoral. The sea-base complex is constantly moving and is defended by naval combatants.

Fast deployment and basing ships (FDBS) are the nucleus of the sea-base complex. Characteristics of this ship, along with a conceptual side and top view, are depicted in Figure 22. The FDBS provides rapid deployment and can serve as a maritime pre-positioning ship. The basic difference between a FDBS and an amphibious ship is that the FDBS is a basing and logistics ship that carries all the elements of floating port infrastructure, while an amphibious ship is a combatant designed for the insertion of troops over-the-shore and in ship-to-objective movements. The FDBS is designed to serve as a multi-purpose ship for rapid transit of joint combat ready units, act as a pre-positioning ship, and act as a basing ship for a sea-base complex.

Landing ship ballasting ramps (LSBR) are the center piece of the advanced tactical support base. The LSBR is the essential part of the advanced tactical support base and the sea-basing complex. It is an advanced over-the-shore capability that can rapidly establish temporary and re-locatable over-the-shore entry points along the littoral. It carries port infrastructure facilities, basing barges (barges with austere basing facilities that can be moored along the shore), and an automatically extended ramp that can be built in sections to the shore (for distances up to a mile). As shown in the conceptual drawing in Figure 23, it ballasts down, grounds and moors off the beach, and extends its ramp. It becomes a "port" pier where FDBS and other ships can come alongside and offload.

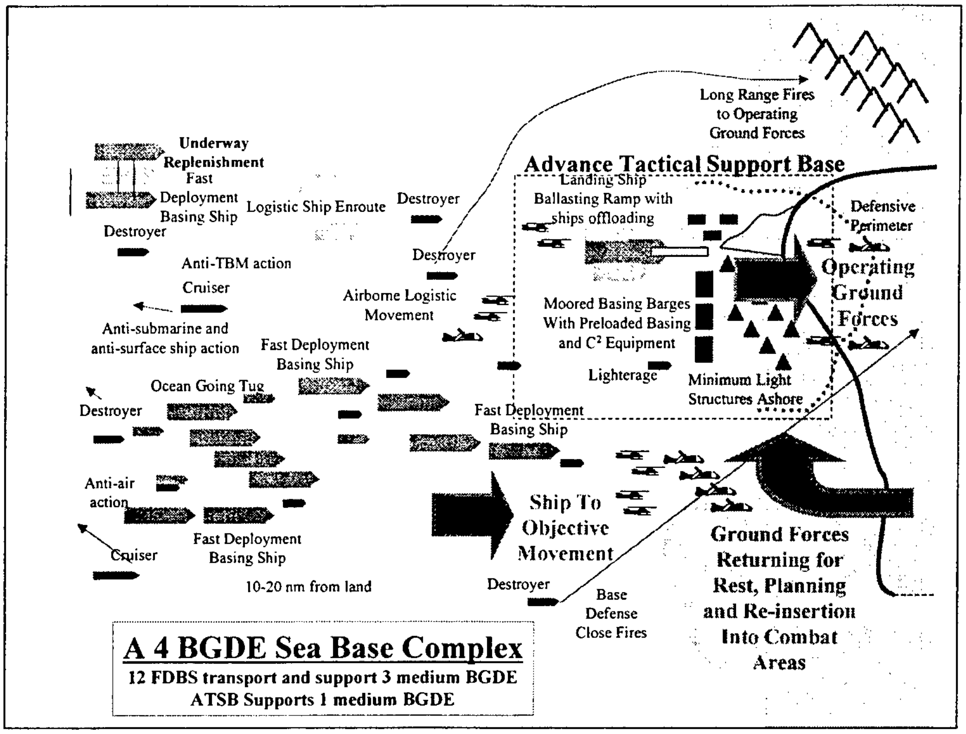


Figure 21. SeaBase Complex and Advanced Tactical Support Base

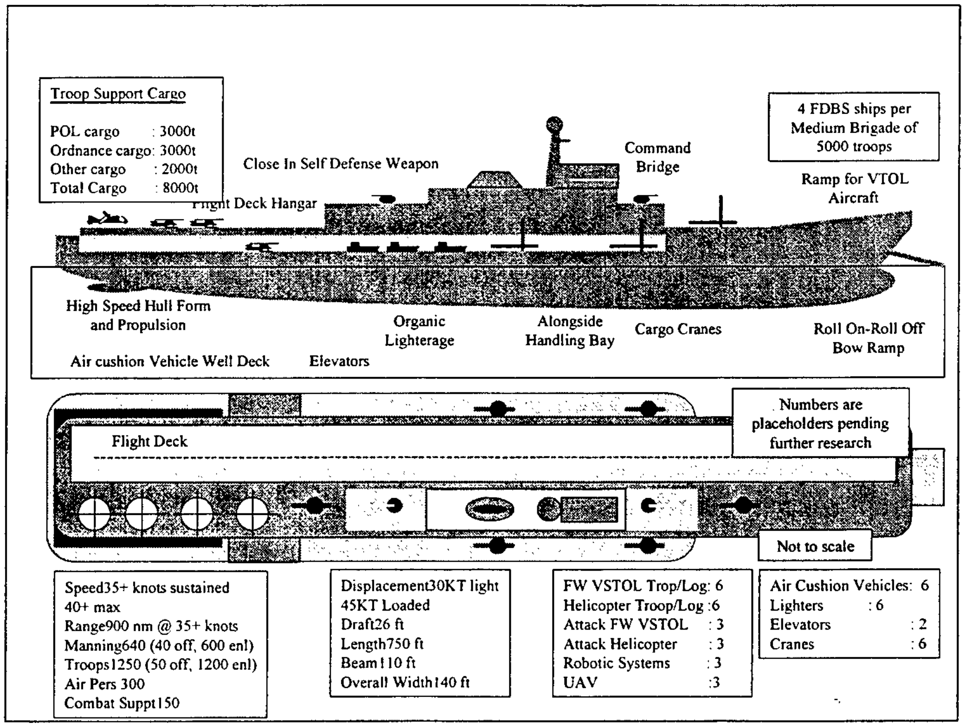
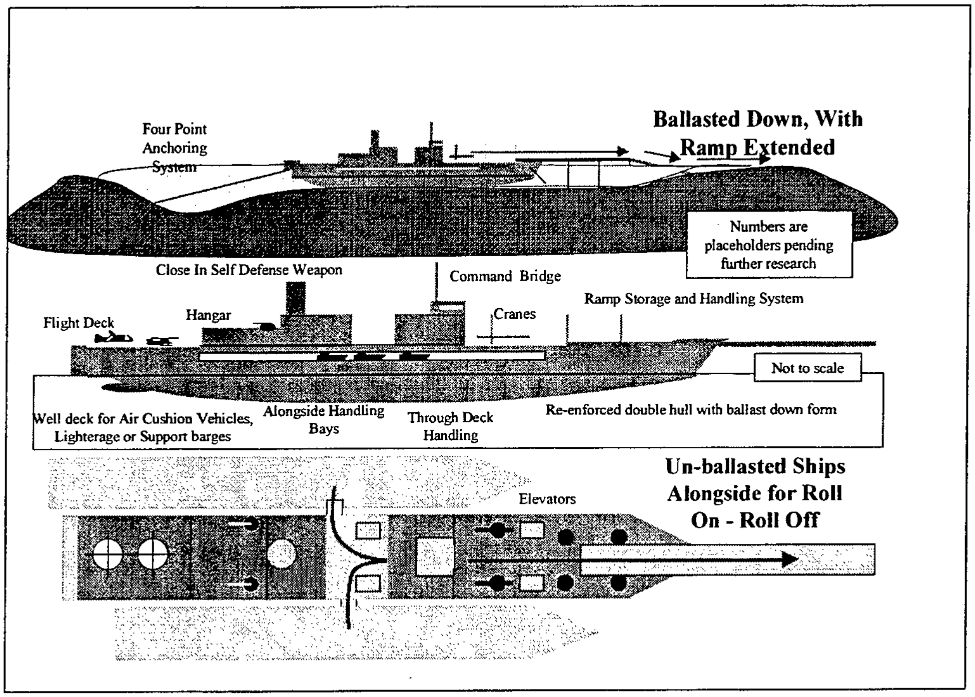


Figure 22. Characteristics of a Fast Deployment and Basing Ship

The FDBS will have the ability to move logistic materiel ashore by VSTOL aircraft and lighterage. However, high volumes of equipment can be rapidly offloaded by ships alongside the LSBR in its ballasted down configuration (essentially a stable pier near the shore, with cranes and other "port" infrastructure). The FDBS are brought into an area protected by naval combatants (local sea and air superiority is established). In the example shown, the result is a four brigade size sea-base complex, associated with and supporting an ATSB. Twelve FDBSs support three medium brigade size joint rapid response operations force (J-ROFs). One brigade (inserted by amphibious or air) is ashore operating from the ATSB.



Four Point Anchoring System
Ballasted Down, With Ramp Extended
Numbers are placeholders pending further research
Close In Self Defense Weapon
Command Bridge
Ramp Storage and Handling System
Flight Deck
Hangar
Cranes
Not to scale
Well deck for Air Cushion Vehicles, Lighterage or Support barges
Alongside Handling Bays
Through Deck Handling
Re-enforced double hull with ballast down form
Elevators
Un-ballasted Ships Alongside for Roll On - Roll Off

Figure 23. Characteristics of a Landing Ship Ballasting Ramp

- The sea base concept for rapid deployment operation suggest the following opportunities: Develop operational requirements and explore development of a Landing Ship Ballasted Ramp providing an advanced over-the-shore capability and the nucleus of an advanced tactical support base.
- Develop operational requirements and explore development of a Fast Deployment and Basing Ship, providing the nucleus of a sea-basing complex as well as providing rapid deployment and a ship for maritime pre-positioning.

COMMERCIAL OPPORTUNITIES

Recent studies by the Defense and Army Science Boards have suggested leveraging oncoming commercial sea and related internodal improvements. Examples of these are high speed ships (HSS-40kt) and agile ports. The basis for previous and current recommendations is that overall commercial trends in sea and related land freight movement are unfavorable for DoD. The U.S. rail industry is consolidating around a few companies and a sparse high-throughput network. DoD forces and supplies will move more slowly to ports because they are not likely to be on the railroad superhighways.

Worldwide trends in sea shipping are toward bigger (6000 TEU) container ships, packaged and fast load-unload cargo, and a reduced number of deep water, high-throughput ports. Neither trend favors DoD. Thus, the Department will have to depend on its own small fleet and the small U.S. fleet of smaller (1000 TEU) ships and ROROs.

The possibility of a fast load-transit-unload ship is therefore a rare favorable circumstance. The DoD should examine and support the incorporation of national defense features for fast load-unload ships, particularly at austere ports for early entry forces. It should also support Title XI loan guarantees. In that same vein, TRANSCOM MSC should leverage, where they are available, high-speed ferries capable of shallow port access. This requires no acquisition but only information and planning tools.

As a final initiative, DARPA and the Army, as Joint Rotorcraft Executive Agent, should incorporate the use of advanced rotorcraft for unloading and loading ships. These capabilities would provide truly uncertain and even transiently occupied insertion points for early entry forces and supplies arriving from the CONUS or forward bases from the sea. These same advanced rotorcraft could also support a number of traditional tactical logistics and mobility missions were they able to lift 70 tons at sea level and lesser amounts under the usual 4000 foot 95 F conditions. Several promising VTOL possibilities currently focused on smaller payloads and different missions should be examined in competitively structured scaling analysis to understand the possibilities and limitations. This should be done by DARPA and the Army.

QUICK REACTION CONUS PREPO

Analyses, conducted by several organizations in this set of studies, show clearly that port-to-port transit time is half or less than the time for total deployment. For legacy forces, which are based in the central portions of the United States, a substantial amount of time is spent generating, moving, and loading the force at ports. In the analyses performed to date, along with actual experience from the Gulf War and other deployments, it might take as much as four to six days, plus preparation time, to move units from Ft. Hood to Gulf ports and load them. Railroads would be the primary means of moving heavy tracked vehicles from interior posts.

An earlier portion of this report cited the character and growth in the U.S. freight and transportation marketplace. In that marketplace, the railroads have been in a state of steady decline for the last 40 years. The interstate highway system has spurred growth in the trucking sector, and airfreight is a steadily growing component. The Army has an opportunity to make a substantial change in deployment time through what might be called a combined active-reserve initiative, one that leverages the historic ability of the states to contribute to national military power.

Recent technological advances in the operational storage of Army equipment also present a significant opportunity for improving the timely projection of heavy forces. The National Guard is making extensive use of controlled humidity preservation (CHP), a storage method that stores equipment in fully mission capable status – ready for immediate deployment – over an extended period of time. The cost of a CHP facility large enough to house the tracked vehicles of a heavy brigade task force is around 3 to 4 million dollars ($24.00 per square foot). In time, the cost of the CHP facility would be recovered by the savings on scheduled and unscheduled maintenance of the housed equipment.

CHP provides an excellent means to store a portion of the on-hand equipment of heavy divisions in an immediately deployable condition. In geographic situations such as that enjoyed by the 3rd Infantry Division, the CHP facility could be located at or within tracked driving distance of the ship loading point. The close proximity to the port would greatly enhance the speed of loading (the estimated task force loading time is less than 48 hours). It would also greatly reduce the potential for hostile disruption and make a visual and physical statement to the American people that the Army is ready to move. In the case of the 3rd Division, the 48th Brigade (if available), Georgia National Guard, and other reserve forces in the area could assist with equipment preparation and ship loading, thereby releasing 3rd Division soldiers for other pre-deployment activities.

An analogous situation applies in the port of Philadelphia which also has the advantage of being modified to become an agile port and home port for an HSS-40 terminus. The 28th Division could place a brigade of its mechanized equipment in the port as CONUS PREPO available for rapid deployment.

To exploit the possibilities resident in delivery to austere ports, funding to add national defense features to ships and ferries should be directed toward improving rapid loading and unloading and austere capabilities for commercial ships, particularly high speed sealift.

Findings are analogous to those for air and include the following:

- Emphasize the exploitation, stimulation, and adaptation to commercial initiatives which have high payoff for the DoD such as high speed sealift with rapid load and unload features. Navy and Army requirements for strategic sealift should be revised to include high speed sealift. The Army, the Navy, and the Department of Transportation should pursue Title XI support for HSS and the incorporation of national defense features (NDF) to support military cargo and austere port operations.

- A combined active and reserve component initiative should be undertaken to save substantial deployment time for Army XXI units in the very near future – concepts to be tested as part of periodic strategic responsiveness exercises. The

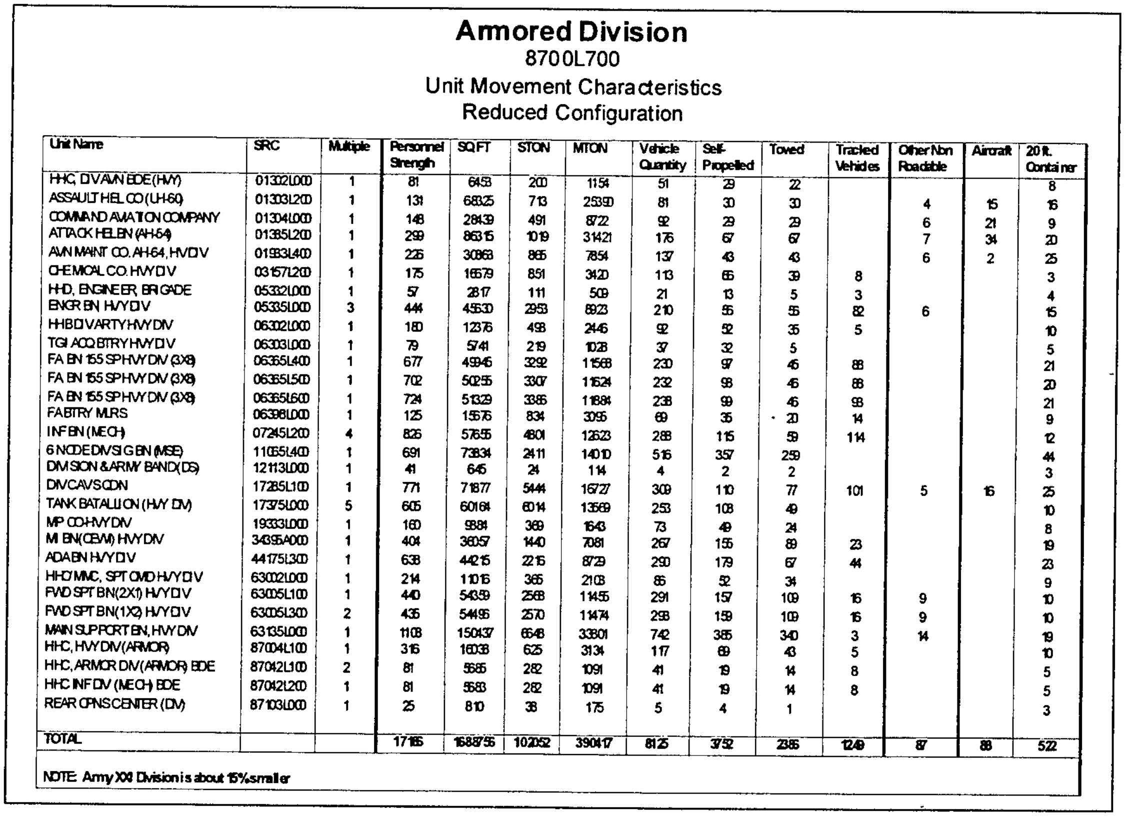
Army should develop an operational concept and report back to the Army Chief of Staff within six months with a formulated plan.

- National defense funding should be focused on rapid loading and unloading and austere capabilities for commercial shipping that would be leveraged by the Army.
- DARPA and the Army should examine the scaling potential in advanced VTOLs for use in austere port unloading.
- The DoD, possibly using the Army as lead Service, should establish and adhere to packaging standards.

ACHIEVING EFFICIENT LAND MOBILITY

Forces will undertake substantial movement on land. Other than reducing numbers, there are limited opportunities for DoD legacy forces to reduce footprint and weight to reduce shipping demand and fuel consumption in theater. The Services have a set of initiatives underway to reduce deployed unit size through reach back, split basing, and similar strategies.

Figure 24 is an example cited from MTMC-TEA Reference 97-700-5 (*Deployment Planning Guide*) database that characterizes the older armored division. This notional armored division has 17,000 men, weighs 100,000 tons, has 8,000 vehicles, and 522 containers. When loaded on ships, or aircraft when possible, it occupies a million and a half square feet. Division equipment includes almost 2,000 tracked vehicles, approximately 4,000 wheeled vehicles, about 2,500 towed vehicles, and nearly 100 aircraft. The weight of the combat platforms, compared to the entire division, results in an operating ratio of about 42 percent. For combat personnel, the ratio is about 24 percent. When deploying larger corps level units, this drops to 15 percent. Virtually all of the overhead is attributed to trucks. Improving trucks and their performance should be a major initiative for all Services.



Armored Division
8700L700
Unit Movement Characteristics
Reduced Configuration

Unit Name	SRC	Multiple	Personnel Strength	SQFT	STON	MTON	Vehicle Quantity	Self-Propelled	Towed	Tracked Vehicles	Other Non Roadable	Aircraft	20 ft. Container
HHC, DIV AVN BDE (HVY)	01302L000	1	81	6458	200	1154	51	29	22				8
ASSAULT HEL CO (UH-60)	01303L200	1	131	68325	713	25390	81	30	30		4	15	16
COMMAND AVIATION COMPANY	01304L000	1	148	28439	491	8722	92	29	29		6	21	9
ATTACK HEL BN (AH-64)	01385L200	1	299	86315	1019	31421	176	67	67		7	34	20
AVN MAINT CO. AH-64, HVY DIV	01983L400	1	226	30863	865	7854	137	43	43		6	2	25
CHEMICAL CO. HVY DIV	03157L200	1	175	16679	851	3420	113	65	39	8			3
HHD, ENGINEER BRIGADE	05332L000	1	57	2817	111	509	21	13	5	3			4
ENGR BN HVY DIV	05335L000	3	444	45530	2953	8923	210	55	55	82	6		15
HHB DIVARTY HVY DIV	06302L000	1	180	12376	498	2446	92	52	35	5			10
TGT ACQ BTRY HVY DIV	06303L000	1	79	5741	219	1028	37	32	5				5
FA BN 155 SP HVY DIV (3X8)	06365L400	1	677	49946	3292	11568	230	97	46	88			21
FA BN 155 SP HVY DIV (3X8)	06365L500	1	702	50255	3307	11624	232	98	46	88			20
FA BN 155 SP HVY DIV (3X8)	06365L600	1	724	51329	3386	11884	238	99	46	98			21
FA BTRY MLRS	06398L000	1	125	15676	834	3095	69	35	20	14			9
INF BN (MECH)	07245L200	4	826	57655	4801	12623	288	115	59	114			12
6 NODE DIV SIG BN (MSE)	11065L400	1	691	73834	2411	14010	516	357	259				44
DIVISION & ARMY BAND (DS)	12113L000	1	41	645	24	114	4	2	2				3
DIV CAV SQDN	17285L100	1	771	71877	5444	16727	309	110	77	101	5	16	25
TANK BATALLION (HVY DIV)	17375L000	5	605	60164	6014	13569	253	108	49				10
MP CO HVY DIV	19333L000	1	160	9884	369	1643	73	49	24				8
MI BN (CEWI) HVY DIV	34395A000	1	404	36057	1440	7081	267	155	89	23			19
ADA BN HVY DIV	44175L300	1	638	44215	2215	8729	290	179	67	44			23
HHC/MMC, SPT CMD HVY DIV	63002L000	1	214	11016	365	2108	86	52	34				9
FWD SPT BN (2X1) HVY DIV	63005L100	1	440	54359	2568	11455	291	157	109	16	9		10
FWD SPT BN (1X2) HVY DIV	63005L300	2	435	54495	2570	11474	298	159	109	16	9		10
MAIN SUPPORT BN, HVY DIV	63135L000	1	1108	150437	6648	33801	742	385	340	3	14		19
HHC, HVY DIV (ARMOR)	87004L100	1	316	16038	625	3134	117	69	43	5			10
HHC, ARMOR DIV (ARMOR) BDE	87042L100	2	81	5685	282	1091	41	19	14	8			5
HHC INF DIV (MECH) BDE	87042L200	1	81	5683	282	1091	41	19	14	8			5
REAR OPNS CENTER (DIV)	87103L000	1	25	810	38	175	5	4	1				3
TOTAL			17166	1688756	102052	390417	8125	3752	2386	1249	87	88	522

NOTE: Army XXI Division is about 15% smaller

Figure 24. Characteristics of a Notional Armored Division

Some fuel efficiency could be derived from the commercial sector movement to hybrid electric drive and ultimately to fuel cell employment for generating electricity for propulsion. The DoD should track these programs carefully. An informal estimate made in 1998 concluded that the Department of Defense was spending possibly $100 million a year in research on propulsion for advanced land vehicles. An informal estimate made by DARPA was that ten major automobile manufacturers were investing something between $2 and 6 billion a year. For example, Toyota recently fielded its first hybrid electric vehicle for evaluation; it will be the first to market.

Another commercial innovation, which could be regarded as a non-developmental item, is called the FLYER. The FLYER is currently being developed along the lines of a truck built structurally like an airplane. It has a very lightweight chassis, which is strong and adequate but avoids the weight excesses that exist in today's designs. FLYER vehicles carry loads equal to or slightly greater than their empty weight as compared to the trucks used by DoD today which carry about half their empty weight. The FLYER also offers vehicle number and crew efficiencies. Shown in Figure 25 are three current Army vehicles [the high-mobility, multi-purpose wheeled vehicle (HMMWV) and two trucks] along with three possible FLYER configurations. The first and lightest of the FLYER vehicles is one which is currently being sold to nations such as Singapore and to the Marine Corps. The heavier versions of the FLYER are engineering estimates – they have not yet been built.

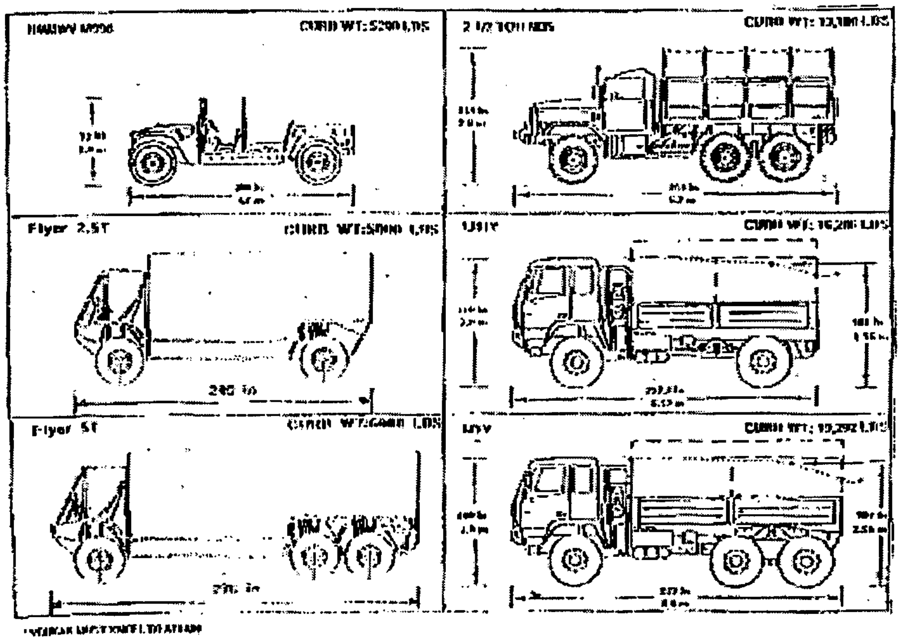


Figure 25. Land Mobility Vehicle Candidates

Overall, there are substantial opportunities to improve efficiency in numbers of vehicles needed, manning, and fuel consumption. This applies throughout DoD.

LOGISTICS CHALLENGES AND IMPROVEMENTS

Many challenges must be addressed in order for the Department to improve its logistics operations to achieve the goals of *Joint Vision 2010*. They include the following:

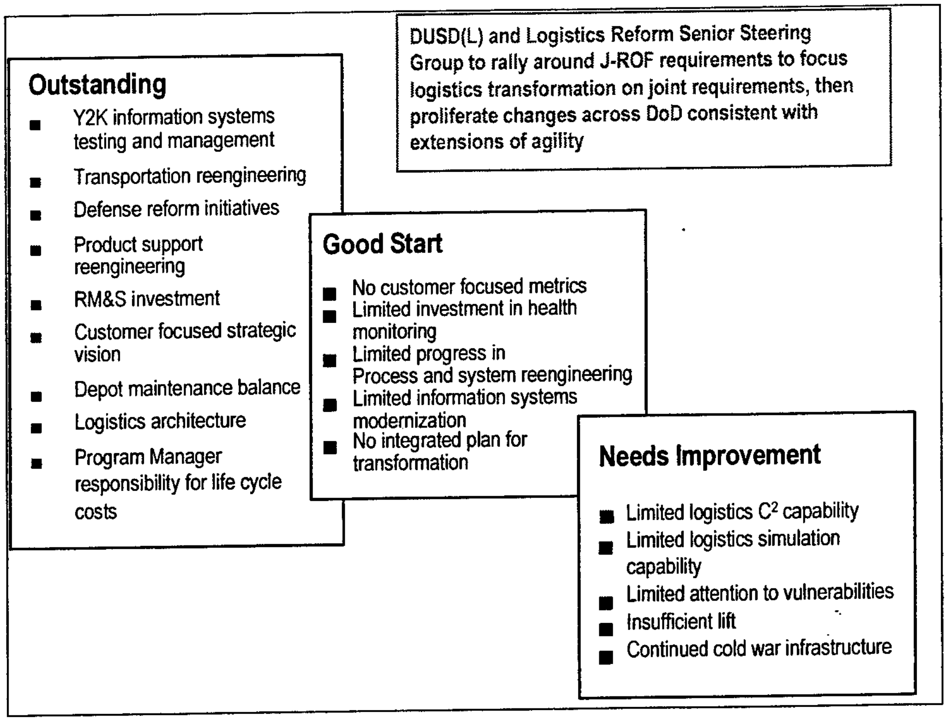
- Managing DoD logistics is a big, complex business
  - Over 5 million stock items
  - 16 inventory control points
  - 19 distribution depots
  - 24 maintenance depots
  - Over a million people
  - $80 billion per year
- J-ROFs present new requirements
  - Agility
  - Interoperability
  - Worldwide, rapid response
  - Higher effectiveness at lower cost
- DoD is addressing many of its logistics challenges
  - Customer focus vision
  - Defense reform initiatives (transportation, cycle time)
  - Product support reengineering
  - Logistics architecture
  - Service and DLA initiatives (300)
- DoD is realizing incremental benefits from transformation and commercial practices
  - Logistics response time down to 18 days
  - Secondary item inventory down 40 percent
  - Strategic lift on target for FY 2003 goals
  - In-storage asset visibility over 90 percent
- However, incremental improvements will not meet the requirements of *Joint Vision 2010*, nor support of the J-ROFs
  - Inappropriate metrics/reward systems and disjointed supply chains
  - Significant infrastructure with multiple nodes
  - Support to fielded systems (spotty readiness)

- Decaying information infrastructure; limited logistics C^2
- Inadequate lift to support rapid response

Recent DoD Logistics Transformation Efforts

There can be no revolution in military affairs without a supporting revolution in military logistics. Enabling effective early entry forces and supporting follow-on forces demands the kind of performance improvements, if not the processes, that have transformed commercial logistics.

The key question is whether improvements to date have been sufficient to support the focused logistics concept described in *Joint Vision 2010*. To assess overall DoD progress in focusing logistics, the 1999 DSB reviewed recommendations made by the 1996 and 1998 DSB studies. In several areas, DoD has realized significant progress. The Department successfully addressed the Year 2000 challenge for over 1000 logistics information systems, completed detailed reengineering transportation transactions, established a logistics architect, and implemented program manager responsibility for life cycle costs as shown in Figure 27. These efforts will continue to dramatically improve DoD logistics performance over the next decade; however, based on prior DSB recommendations, DoD still has several areas that require attention.



DUSD(L) and Logistics Reform Senior Steering Group to rally around J-ROF requirements to focus logistics transformation on joint requirements, then proliferate changes across DoD consistent with extensions of agility

Outstanding

- Y2K information systems testing and management
- Transportation reengineering
- Defense reform initiatives
- Product support reengineering
- RM&S investment
- Customer focused strategic vision
- Depot maintenance balance
- Logistics architecture
- Program Manager responsibility for life cycle costs

Good Start

- No customer focused metrics
- Limited investment in health monitoring
- Limited progress in Process and system reengineering
- Limited information systems modernization
- No integrated plan for transformation

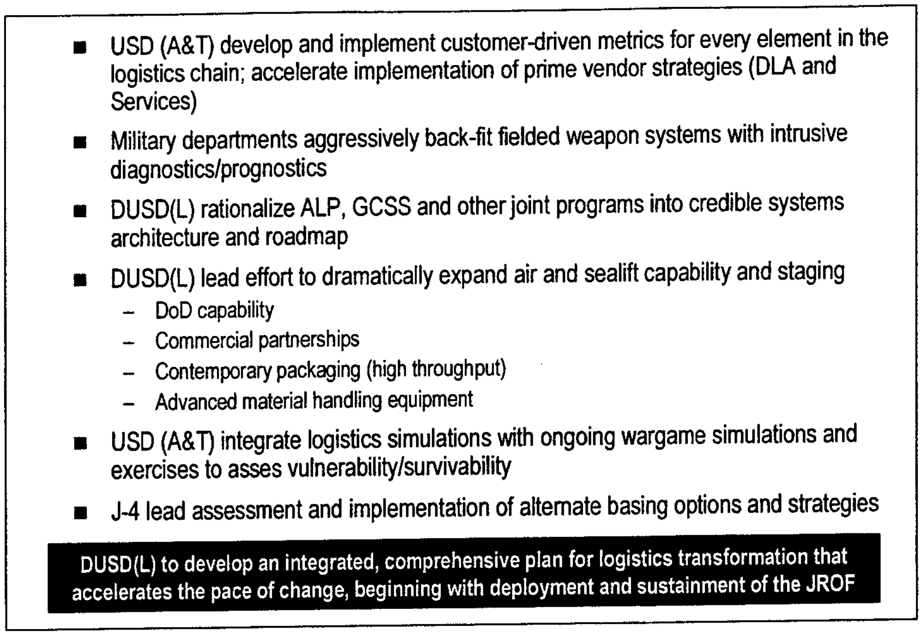
Needs Improvement

- Limited logistics C^2 capability
- Limited logistics simulation capability
- Limited attention to vulnerabilities
- Insufficient lift
- Continued cold war infrastructure

Figure 26. Recent DoD Logistics Transformation Efforts

For example, a common customer-focused vision was a major step forward, but to improve customer responsiveness, metrics for every node in the supply chain must be developed and implemented. Similarly, because of the appropriate focus on Y2K, DoD has done little in the area of systems modernization and associated process reengineering. Finally, as recommended in the 1998 DSB Summer Study, the Department lacks an integrated plan to transform logistics. Similarly, adopting advanced information systems and simulation has been slow. DoD has not aggressively addressed potential vulnerability of its logistics system nor its existing CONUS-based system infrastructure. Finally, although the Department is on track to meet its lift requirements (over a sustained period), current strategic lift capacity is inadequate to meet the surge requirements of a J-ROF. Commercial solutions are a necessity.

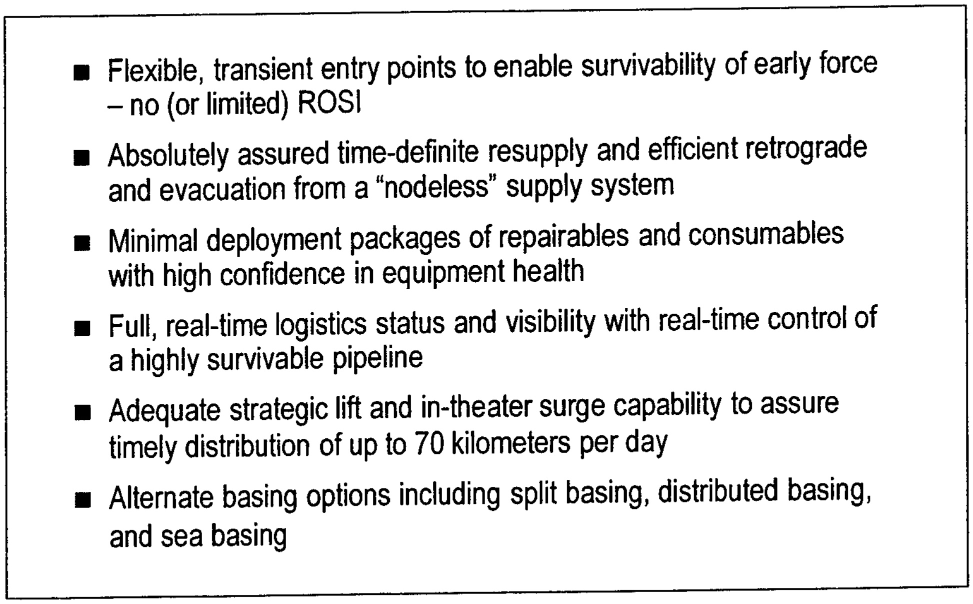
To address these areas and to accelerate the pace of change within DoD logistics, the task force offers several strategic actions as described in Figure 27. First, the Under Secretary of Defense for Acquisition and Technology [USD(A&T)], through the Deputy Under Secretary of Defense for Logistics [DUSD(L)] and the logistics architect, should develop and implement customer-driven metrics for every node in the supply chain. DUSD(L), in conjunction with the Under Secretary of Defense for Personnel and Readiness [USD(P&R)] should translate these metrics into personnel evaluation criteria and performance awards for logistics managers. DLA should accelerate its efforts with corporate partnering and prime vendor strategies and with existing demonstrations of infusing prognostics on all major platforms. The DUSD(L) should immediately address information systems modernization, beginning with a roadmap for the Advanced Logistics Program, the Global Combat Support System (GCSS), and other joint programs. DUSD(L) should initiate a focusèd effort, in conjunction with J-4 and TRANSCOM, to enhance strategic mobility. USD(A&T), through the DUSD(L), should capitalize on recent logistics simulations (Y2K and TRANSCOM), to incorporate those efforts into wargame exercises. Finally, the J-4 should lead an assessment of alternative basing options and strategies including split-basing, joint-basing, and all-basing. The DUSD(L), in conjunction with the Logistics Reform Senior Steering Group, should integrate these actions into a comprehensive plan that accelerates logistics transformation to meet the sustainment requirements of the J-ROF, as shown in Figure 28.



- USD (A&T) develop and implement customer-driven metrics for every element in the logistics chain; accelerate implementation of prime vendor strategies (DLA and Services)
- Military departments aggressively back-fit fielded weapon systems with intrusive diagnostics/prognostics
- DUSD(L) rationalize ALP, GCSS and other joint programs into credible systems architecture and roadmap
- DUSD(L) lead effort to dramatically expand air and sealift capability and staging
  - DoD capability
  - Commercial partnerships
  - Contemporary packaging (high throughput)
  - Advanced material handling equipment
- USD (A&T) integrate logistics simulations with ongoing wargame simulations and exercises to asses vulnerability/survivability
- J-4 lead assessment and implementation of alternate basing options and strategies

DUSD(L) to develop an integrated, comprehensive plan for logistics transformation that accelerates the pace of change, beginning with deployment and sustainment of the JROF

Figure 27. Strategic Logistics Transformation Actions Required



- Flexible, transient entry points to enable survivability of early force – no (or limited) ROSI
- Absolutely assured time-definite resupply and efficient retrograde and evacuation from a "nodeless" supply system
- Minimal deployment packages of repairables and consumables with high confidence in equipment health
- Full, real-time logistics status and visibility with real-time control of a highly survivable pipeline
- Adequate strategic lift and in-theater surge capability to assure timely distribution of up to 70 kilometers per day
- Alternate basing options including split basing, distributed basing, and sea basing

Figure 28. J-ROF Sustainment Needs

These strategic actions should be focused initially to meet the need of the J-ROF, so that reengineered or logistics process and sustainment concepts can be evaluated during J-ROF experimentation. Key elements of the J-ROF sustainment requirements include flexible, transient entry point, with limited RSOI required. If the J-ROF deploys with a 5-day sustainment package, that force must be assured of time-definite re-supply from a survivable, nodeless supply system. To increase agility, the J-ROF must deploy with minimal spares and maintenance packages, yet with a high degree of confidence in the health of their systems. To enhance sustainment, the J-ROF commander must have full, real-time logistics awareness and control of the pipeline. Following initial deployment, sufficient strategic and in-theater lift is needed to re-supply the deployed force. Finally, to enhance J-ROF survivability, the force requires alternate basing options that minimize footprint and enhance agility.

Fortunately, the USD(A&T) recently published a report on reengineering product support. The primary focus was to improve weapon system readiness through increased reliance on CONUS-based integrated supply chains as illustrated in Figure 29. The reengineered process will be implemented and tested first on 30 high-cost pilot programs, as shown in Figure 30, then across all major platforms. The product support pilot programs include high cost, high visibility platforms across the military departments. The military departments are preparing detailed product support strategies for review by USD(A&T) by mid October 1999.

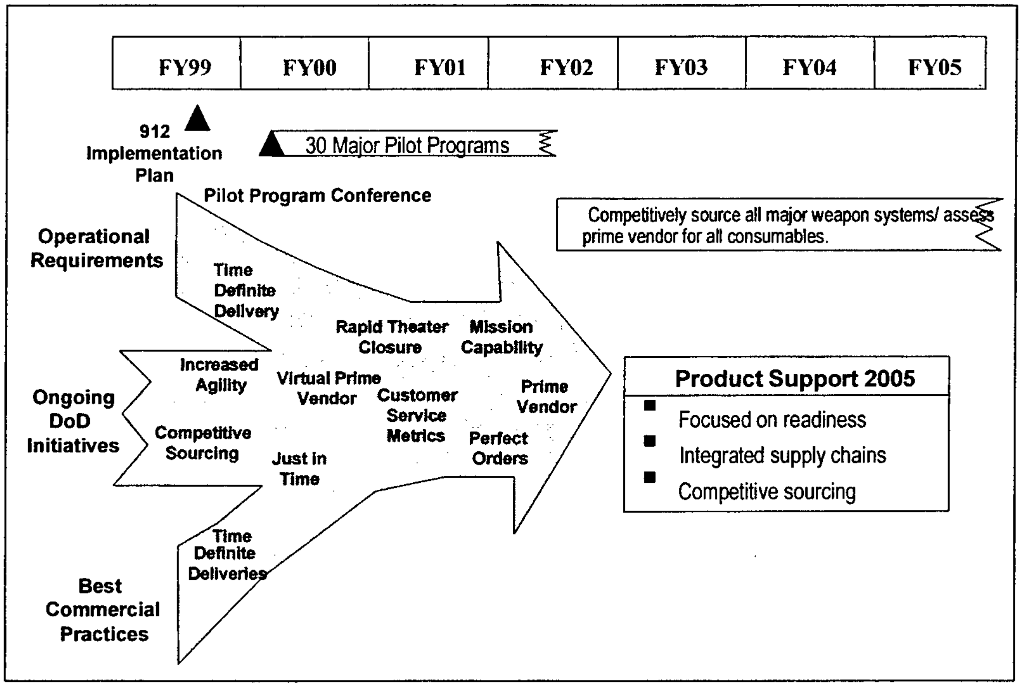
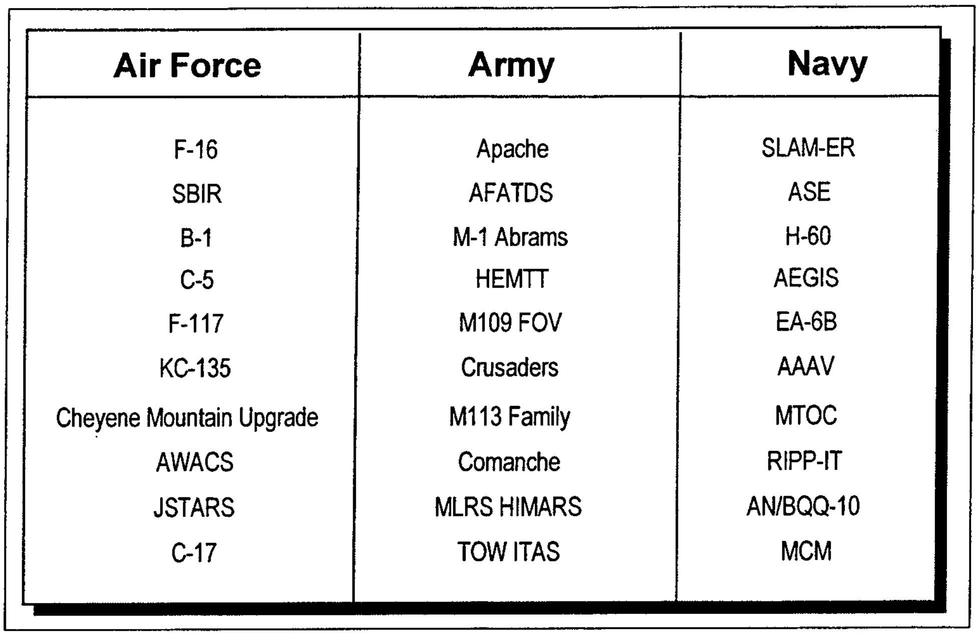


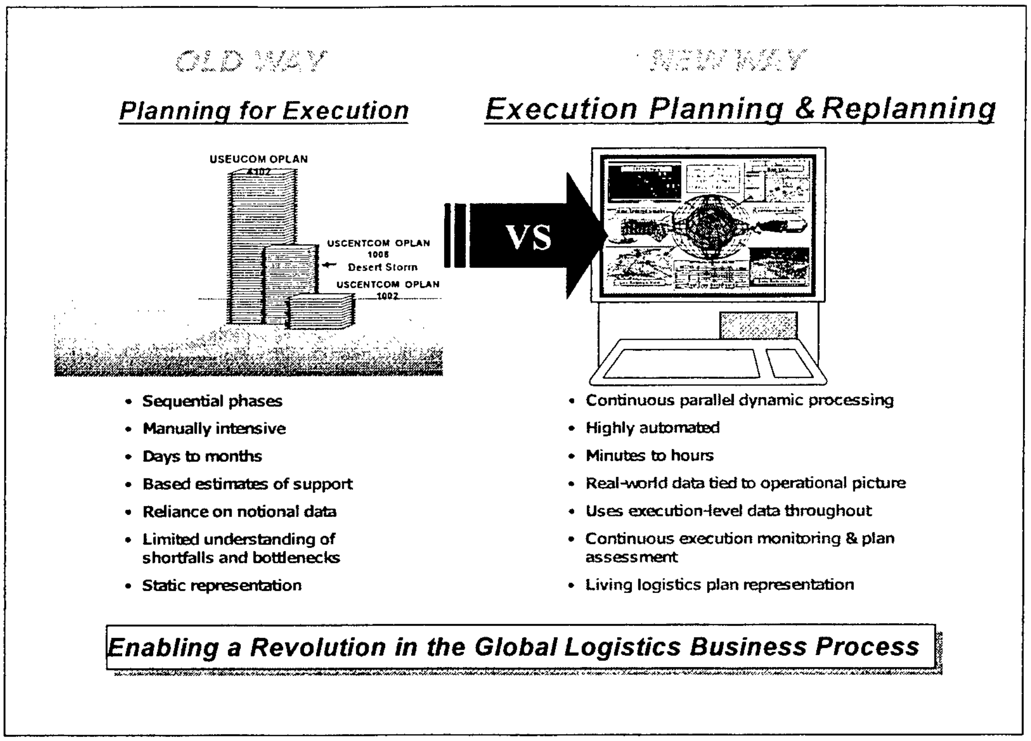
Figure 29. Reengineer Product Support



Air Force	Army	Navy
F-16	Apache	SLAM-ER
SBIR	AFATDS	ASE
B-1	M-1 Abrams	H-60
C-5	HEMTT	AEGIS
F-117	M109 FOV	EA-6B
KC-135	Crusaders	AAAV
Cheyene Mountain Upgrade	M113 Family	MTOC
AWACS	Comanche	RIPP-IT
JSTARS	MLRS HIMARS	AN/BQQ-10
C-17	TOW ITAS	MCM

Figure 30. Thirty Pilot Programs: Testing Alternative Strategies

One of the key elements of focused logistics is the ability to rapidly plan and replan logistics support based upon dynamic operational needs. Previously, the logistics support portion of a Commander-in-Chief's (CINC) operations plan was developed manually, in sequential phases, and often involved several months, shown in Figure 31. In response to this limitation, the Defense Advanced Research Projects Agency initiated the Advanced Logistics Program to assess and demonstrate the value of advanced information technology, object-oriented technologies, and smart agents to dramatically reduce the planning and replanning cycle.



OLD WAY

Planning for Execution

- Sequential phases
- Manually intensive
- Days to months
- Based estimates of support
- Reliance on notional data
- Limited understanding of shortfalls and bottlenecks
- Static representation

NEW WAY

Execution Planning & Replanning

- Continuous parallel dynamic processing
- Highly automated
- Minutes to hours
- Real-world data tied to operational picture
- Uses execution-level data throughout
- Continuous execution monitoring & plan assessment
- Living logistics plan representation

Enabling a Revolution in the Global Logistics Business Process

Figure 31. Achieving Focused Logistics

BENEFITS OF SCIENCE AND TECHNOLOGY GRAND CHALLENGES

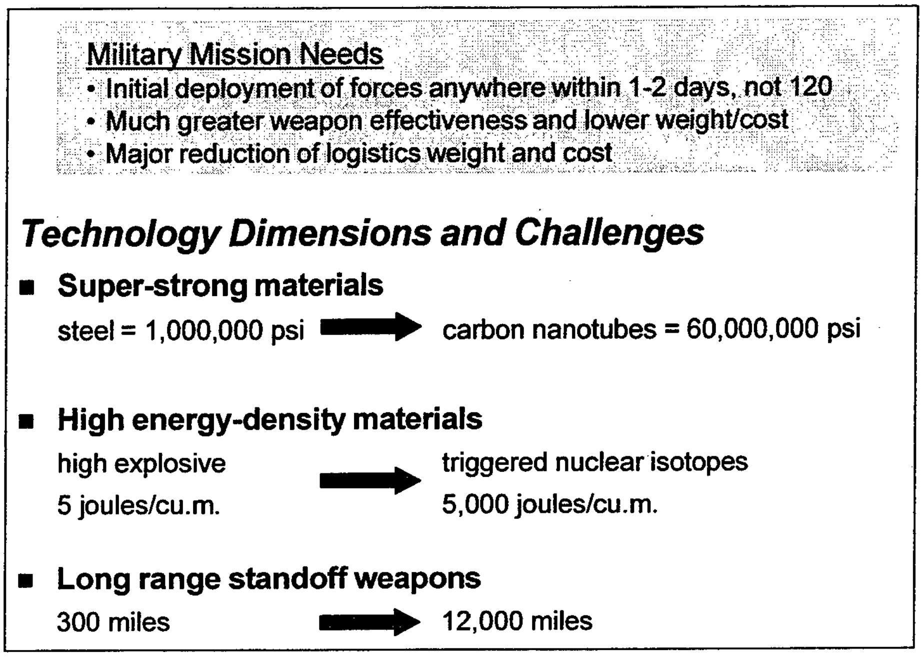
The DoD has gone through a series of significant changes since the end of World War II. Driven by new concepts and new technologies which were the subject of pre-war study and preparations, changes were implemented very rapidly while the war itself was being prosecuted. Examples of these were the emergence of the battle group built around the aircraft carrier developed by both the United States and Japan; in land warfare, the Blitzkrieg developed by the Germans; and versions of highly mobile armored formations executing concepts developed by the United States, Britain, and Russia.

Emerging from the war were strategic and theater nuclear weapons and forces and a variety of related concepts, most notably deterrence. In the 70s and 80s, new concepts and conventional technologies were introduced to both enhance deterrence and defense and to reduce the need for an early resort to nuclear weapons use.

Today, the United States enters a new era which requires expeditionary concepts with sufficient strategic agility to deny enemy set. To achieve the desired result will require orders-of-magnitude improvements in current capabilities. To focus science and technology investment, the task force identified "grand challenges" that would dramatically improve early entry capabilities, including sustainment. Characteristics of grand challenge military capabilities include:

- Militarily significant – the basis for enhancing or fundamentally changing military operations
- Quantum jump in performance (at least 10x increase in performance)
- Driver for technology development
- Challenging but feasible (no magic needed)
- Defined objective with measurable, intermediate stages of progress
- Likely unmatchable by adversaries (either costly or time consuming to do so)

Examples of improvements that would enable greater agility are shown in Figure 33. The early entry force, to be effective in denying "enemy set," must be inserted by air and from the sea into unexpected and unpredictable locations. Fortunately, DoD has developed and has current "last mile" air capabilities. Lighter vehicles must have high weapons lethality, mobility, and survivability. Stronger materials, greater propulsion efficiency, and adequate lethality mechanism make it possible to meet these needs. DoD and commercial ships require prepared seaports. Lighter vehicles and systems could also be unloaded by rotorcraft from ships rather than going over the beach. As addressed earlier, rotorcraft with 20-ton lift capability are needed to meet this requirement. Figure 33 describes some of these capabilities in greater detail.



Military Mission Needs

- Initial deployment of forces anywhere within 1-2 days, not 120
- Much greater weapon effectiveness and lower weight/cost
- Major reduction of logistics weight and cost

Technology Dimensions and Challenges

- **Super-strong materials**

  steel = 1,000,000 psi → carbon nanotubes = 60,000,000 psi

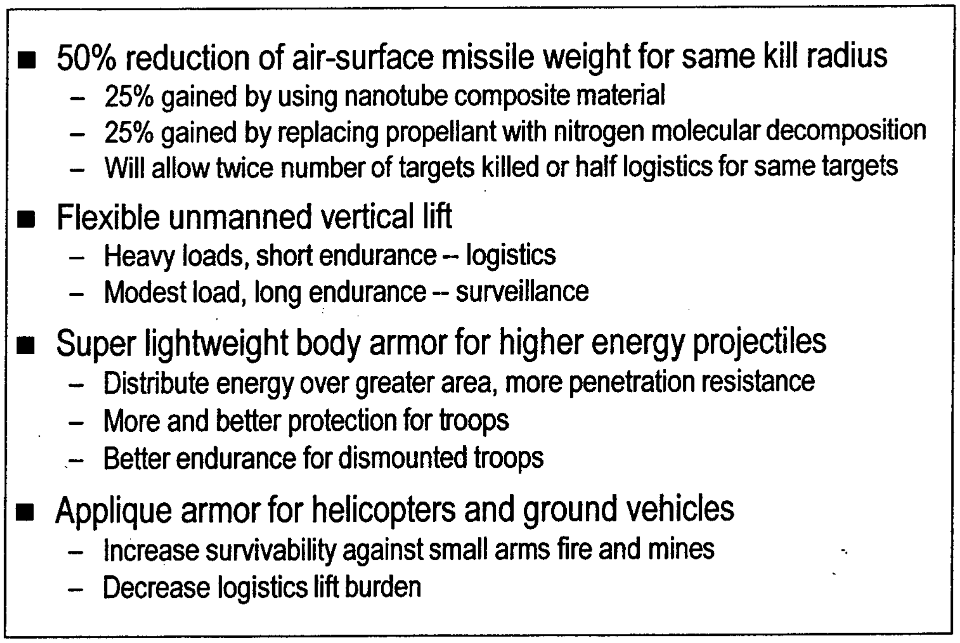
- **High energy-density materials**

  high explosive 5 joules/cu.m. → triggered nuclear isotopes 5,000 joules/cu.m.

- **Long range standoff weapons**

  300 miles → 12,000 miles

Figure 32. Fast Forward



- 50% reduction of air-surface missile weight for same kill radius
  - 25% gained by using nanotube composite material
  - 25% gained by replacing propellant with nitrogen molecular decomposition
  - Will allow twice number of targets killed or half logistics for same targets
- Flexible unmanned vertical lift
  - Heavy loads, short endurance -- logistics
  - Modest load, long endurance -- surveillance
- Super lightweight body armor for higher energy projectiles
  - Distribute energy over greater area, more penetration resistance
  - More and better protection for troops
  - Better endurance for dismounted troops
- Applique armor for helicopters and ground vehicles
  - Increase survivability against small arms fire and mines
  - Decrease logistics lift burden

Figure 33. "Fast Forward" Strategic Agility – Example Intermediate Outputs (5 years)

The benefits gained from the advanced capabilities suggested are also realized in other domains including strategic mobility; handling and transfer (much commercial cargo of 10 to 20 tons is regularly handled by air freight); logistics and sustainment; and force protection.

What are the advantages in reducing missile weight? The example shown in Figure 33 is developed from analysis of today's air-to-surface missiles. It is judged that similar improvements would apply to:

- Air-to-air missiles
- Shoulder launched infantry missiles and anti-armor, anti-structure and antiaircraft
- Vehicle-carried missiles for ground combat.

Possibilities also exist for lighter vehicles and some efficient propulsion and explosives they include:

- Super strong materials: carbon nanotubes
- High energy density materials: multi-stable states of combustion products
- Greater energy efficiency: propulsion
- Combinations of the above for standoff missiles: Low-Cost Autonomous Attack System (LOCAAS), Multiple Launch Rocket System (MLRS)
- Combinations of the above for self-deploying, heavy lift rotorcraft

While a factor of two improvement seems modest, it has a profound infrastructure effect. It reduces rearming frequency by a factor of two. It reduces logistic loads of these weapons by a factor of two. It reduces manpower requirements. All joint force elements have "high overhead." When combined, factors of two can result in profound reductions.

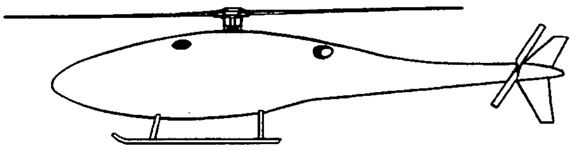
The same effect is realized in protection technology for people and platforms. Better protection enables greater freedom of movement individually and greater freedom of force maneuver as well. Fewer people are injured or killed. Fewer platforms are lost. Again, seemingly modest capabilities of two, three, or four times improvement have profound force endurance benefits and lead to major infrastructure reductions in areas such as replacements, repairs, and hospitals.

DARPA has in development a program called "Hummingbird." While other rotorcraft research is underway, this program is a traditional high-risk, high pay off DARPA program. Unlike its more traditional and evolutionary counterpart, the Joint Tactical Rotorcraft Program, this program reaches for scalability and efficiencies which rival fixed wing aircraft performance as well as unmanned, commandable self-deployable operations.

As indicated in Figure 34, this program has achieved its initial performance milestones in the unmanned domain and should be supported to achieve its endurance and scalability goals as well. The additional benefits of a Hummingbird success include:

- Use in forward area with support based at substantial distance
- Endurance as a platform for sensing, situation awareness, and communication relay
- A logistics transport vehicle requiring no forward sustainment or people
- A ship-based fire support platform
- A platform to recover damaged vehicles from terrain too difficult for recovery using ground vehicles
- A warfare vertical transfer vehicle for military operation in urban terrain (MOUT)

This is a modest sample of what might be realized with the Hummingbird program, resulting from successfully applying the materials and high efficiency propulsion realized from a "grand challenge" initiative.



Performance

Range:	**>3000nm**
Endurance:	**>40 hrs**
Payload:	**>300 lbs**

Applications

- **Battlefield Surveillance**
- **Close-In-Sensors relay**
- **Small Unit Re-supply**
- **Combat SAR**
- **Rotor Technology Scaleable to heavy cargo lift (20 ton payload, 1000nm radius)**

Advantages

- **Self-ferry from CONUS**
- **Organic battlefield use without forward logistic burden**

Figure 34. Hummingbird Warrior – Unmanned VTOL

NEEDED IMPROVEMENTS AND RECOMMENDATIONS

This report posited a series of challenges for which solutions were offered. It is important to remember that solutions must apply in an integrated manner in order to gain the benefits of interactions and interdependencies. To recap, these challenges include:

- Improve speed and precision of planning, scheduling, and related front-end processes
- Develop an improved, combined deployment-employment process which is effective and robust when facing a thinking opponent
- Improve airlift, fast sea lift, nodal transfer capability, and intermediate staging based capabilities
- Package forces and supplies for high throughput
- Develop modern combat and support platforms which leverage broadest lift fleets available, and provide needed lethality, tactical/operational mobility, and survivability with substantially reduced sustainment requirements
- Change sustainment concept and system to meet continuing force requirements and reduce/eliminate actions/attacks by a thinking enemy

The precision and timelines of the overall deployment command control will be dramatically improved with a successful ALP development and transition to joint and Service use. ALP has the added advantage of being able to accommodate and employ best-of-breed DoD and commercial software systems. The recommended solutions, improvements, and initiatives for early entry forces are summarized below.

For disrupted or opposed entry circumstances DoD should adopt a combined air and sea deployment concept employing commercial and military assets (and processes) to maximize lift and throughput. It should employ intermediate staging bases fed by commercial airlift in series with military airlift (C-17 and C-130 and their follow-on fleets in the future) to assure entry at austere and unpredictable locations rather than existing airfields. Forces will emerge from their lift platforms ready to fight. There will be little or no RSOI required initially. This concept could be implemented when ports have been secured and defended. In benign circumstances, both DoD and commercial air fleet could be employed in parallel if adequate airfields are available.

Sea-delivered forces will use austere and unpredictable entry locations as well. Neither DoD nor commercial sea lift has austere entry, fast unload features. A suggested capability is an advanced high-efficiency rotorcraft to unload forces and supplies although other possibilities deserve attention.

Logistics would be provided by air for early entry forces or from nearby sea basing if it is available. The DoD must underwrite a non-traditional logistics process, which is not fixed and nodal and configured on interior lines for its high agility early entry Army and Marine ground forces. Its nearby based tactical forces will need similar sustainment until force protection capabilities make safe not only their bases but also the sustainment lines of communications which are provided by the Army.

Timely assured early entry by air will be enabled by parallel use of DoD and commercial airlift and its related process elements in benign cases. For disrupted cases, the special capabilities of DoD fixed and rotary wing aircraft enable assured entry from staging bases and provide movement for the "last mile."

To efficiently employ both sets of assets to full advantage, platforms and supplies must be constrained in weight to 10 tons and shapes consistent with 20'x8'x8' volumes whether containers are used or not. It is possible that a 20-ton limit might apply but those choices must be supported by analysis and testing. The 20-ton choice will create a need for an advanced rotorcraft.

To improve early entry from the sea, the HHS-40 (40kts high speed ship) with rapid load-unload capability presents an opportunity to gain needed capability and minimize cost of acquisition and ownership. National defense features could provide austere port, rapid unload capability. High-speed ferries are becoming more available commercially in the Mediterranean and on the eastern Asian rim. DoD's JLOTS capability is limited.

New DoD capabilities could include a Mobile Offshore Base and a ship family which could include sustainment from the sea without developed or even austere ports.

Unmanned robotic platforms offer a number of useful advantages for both early-entry and follow-on legacy forces. Footprints and numbers of personnel can be reduced. Care in design will have to be given to not only achieving unmanned platform performance but also reducing personnel and support demands and making all compatible with high speed air and sea shipping and transfer.

Finally, leveraging U.S. (and possibly allied) commercial strengths requires the establishment of strategic partnerships. The current policies, regulations, and relationships must be broadened to emphasize collaboration as well as the more traditional CRAF and VISA programs.

The DARPA "virtual airline" program, which is derived from the Federal Aviation Administration collaborative decision making program, shows great promise as one medium to support a true partnership program. It should be extended to air, sea, and land freight, built on its air passenger success.

Logistics improvements applied in CONUS (such as warehousing, tracking, just-in-time) must be carried forward into the theater. Early entry forces will need logistics which support agility and have their own survivability based on non-nodal concepts for operation on non-interior lines. The additional needed improvements resident in achieving a useful and efficient "revolution in military logistics" requires process improvements, which benefit early entry and follow-on forces.

RECOMMENDATIONS

The following recommendations of the Force Modernization task force are based upon the solutions proposed to address the challenges and problems described at beginning of this report. The brief summary of each recommendation includes:

- A summary of its intended purpose
- The proposed action – person, office, or agency responsible for implementation
- The time frame for action

I. *Improve the precision and timelines of deployment-employment planning and scheduling processes.*

What: Plan and arrange for a transition of a successful ALP program from DARPA to an Army-led consortium including TRANSOM, the Navy, and the Air Force.

Who: Director, DARPA; J-4; and Vice Chief of Staff, Army

When: Prepare, plan, and coordinate by 2nd quarter of 2000. Prepare for transition in appropriate Service and joint development program.

II. *Develop a robust deployment-employment process*

- Account for thinking and asymmetrically-armed enemy
- Provide balanced force protection across CINC zones of responsibility
- Assure timely access which is uncertain (locations & times) for enemy
- Maximize effective use of commercial and DoD assets
- Design concept, organization, and resourcing for ISBs
- Design a logistics system for early entry forces to operate without interior protected lines

Who: U.S. Joint Forces Command head process design consortium including TRANSCOM, Army Training and Doctrine Command, Marine Corps Marine Corps Doctrine Education Center, Air Force Air Combat Command, and PNAV.

- Examine in a JWCA environment
- Bring in industry (including commercial)
- Test design(s) against red teams in design and exercises
- Task TRANSCOM for databases for austere entry locations

When: Initiate actions in 4th quarter of 1999. Initiate JWCA in 4th quarter of 2000. Promulgate doctrine 4th quarter of 2001.

III. Commercial Partnerships

What: A sophisticated set of internal DoD and commercial industry outreach actions is needed

- Expansion of DARPA virtual airline activity to include freight, sea and rail systems (and possibly Allies)
- Traditional airfreight national defense features
- Innovative airlift stimulation and NDF
- NDF for HHS-40 for austere parts
- Applique for DoD and commercial ship austere port capability
- C^2 arrangements for collaborative decision making

Who: USD(A&T) should establish an action and oversight group to assure success. It should include the Joint Chiefs of Staff, TRANSCOM, and the Services

When: Establish group by 2Q 2000. Undertake most critical actions during FY 2000.

IV. Packaging

What: DoD should improve its packaging and modularity to enhance its deployment speed and sustainment efficiency. Commercial standards, tactics, techniques, and procedures should be applied to achieve major throughput time and labor savings.

Who: USD (A&T) should designate the Army to be the Executive Agent for this activity.

When: Undertake in 2000 to develop doctrine, tactics, and procedures for application within one year.

V. Modification of existing platforms and systems and research and development of future platforms and systems for Early Entry Missions

What: The early entry concepts treated previously place great premium on highly lethal, mobile and survivable systems with reduced logistics and overall manning overhead. Such enhancements and developments must underwrite the massing of effects through an integration of fires, maneuver, sustainment, and relentless operational tempo directed by command and control with layered intelligence, surveillance, and reconnaissance capabilities, including unit organic means. Technologically, emphasis should be given to network centric force integration and unmanned and manned systems whose reach and influence can be enhanced with robotics. Thus the recommendations are focussed on these developments, as they could enhance both early entry and follow-on forces.

Early entry forces can benefit from traditional commercial airlift throughput capabilities and from non-traditional airlift and sealift capabilities. They must however conform to the standards and constraints that make such commercial capabilities competitively viable. In summary they are:

- For airlift, weight of 10 tons within volumes of 20'x8'x8'. It might be possible to increase the weight up to 20 tons if analysis and testing to be done confirm this limit.
- For sealift, weights of 20 tons within 20'x8'x8' volumes. This seems unusual and unwarranted but it is necessary. Within these limits, ships can be unloaded with rotorcraft and thus provide unpredictable and assured entry.

In the context of the foregoing, the following is recommended:

Army

- Aggressively pursue Advanced Fire Support System (AFSS) with DARPA
- Aggressively pursue Multi-mission Combat System (MMCS) development program with DARPA.
- Direct the Joint Rotorcraft program toward the objectives cited above to provide early entry and tactical mobility for MMCS and legacy forces which meet the weight volume envelop discussed. Early scaling studies should be undertaken in conjunction with DARPA.
- Modernize the 2nd Armored cavalry regiment with available equipment which will substantially change it into a highly lethal and mobile force with substantially more sustainability than current light forces.
- Expand the Division Partnership program to include CONUS in-port basing of some National Guard Brigade equipment sets for rapid deployment by sea and traditional RSOI in theater with active units. National Guard forces will assist in force projection and will then fall in on the equipment of the active brigade initially deployed.

Air Force

- Pursue the Unmanned Combat Air Vehicle (UCAV) program and assure its transportability on commercial and military airfreighters
- Pursue the 250-pound and 500-pound precision bomb programs and acquire inventories. Package these for both commercial shipping and handling from depots through tactical bases

Marines

- Pursue the Reconnaissance, Surveillance, and Target Acquisition (RSTA) Program and improvements to sea basing envisioned in MPR 2010

Navy

- Assure C^4ISR interfaces to tactical ground forces from DD-21

DARPA

- Give priority to C^4ISR development which improve organic ISR for small units and the network capabilities of the small units and the large force. Examples are:
  - Discoverer II
  - Hummingbird along with C^4ISR means such as moving target indication and synthetic aperature radars
  - Austere port unloading technology
  - Dispensable sensors and tags
  - Studies and experiments to demonstrate Hummingbird and other innovative rotorcraft scaling to 20-ton lift capability

Who: The USD(A&T) should task the DDR&E and the DARPA Director to provide a yearly review of programs and resource allocation focused on development for early entry forces.

When: First review should take place in the Spring of 2000

VI. *Logistics and Sustainment*

What: Early entry forces will need a non-traditional logistics system to enhance their agility. New joint and multi-Service concepts are needed to lead to these capabilities.

Who: U.S. Joint Forces Command should form a consortium with the Services to develop, test, and validate the concept and related tactics, techniques and procedures (TTPs).

When: Start process in 1st quarter of 2000. Dialog concept development in one year.

VII. *Additional Logistics Improvements*

What: The joint and service logistics infrastructure is being made more efficient through a series of re-engineering business process and information systems and technology appliques. Much remains to be done. It is a high payoff but long-term venture. All are encouraged and described in the Annex to the report. Two areas are suggested for examination that would include experimentation. The first has to do with trucks – the DoD's most pervasive platforms. The second has to do with energy generation.

New high-payload efficiency trucks are now becoming available as a result of developments for foreign sales and purchases of test samples by the Marines. This development should be examined for its long-term payoff possibilities because it reduces fleet size, spare inventories, fuel usage, and manning for both direct and support.

Who: The USD (A&T) should task the DUSD(L) to provide an assessment of the possibilities in future truck acquisitions and plan of action to make these possibilities a reality.

Energy generation is usually provided with traditional tiered commercial generators. All the Services which operate on land have large numbers. An armored division has about 1500, for example. The action recommended is that the DUSD(L) and the Director, Defense Research and Engineering undertake an assessment and planning activity to determine when the micro electro mechanical systems (MEMS) research, which DoD has funded, will reach manufacturing maturity. They should then develop a plan for a changeover in acquisition to MEMS-based power generation which offers great acquisition and ownership reduction in cost.

When: The studies and planning should be completed by the end of 2000.

IX. Commercially Based Deployment Exercises

What: Deployment exercises are conducted regularly for all Service forces. Rather than supporting them with DoD assets (lift, handling, information management, tracking, planning) the Department should employ principally commercial capabilities. This will provide a better understanding of how to use these increasingly important capabilities and develop information relative to partnering.

Who: U.S. Joint Forces Command has the lead for such joint undertakings and should modify or expand planned deployment exercises for the stated purposes.

When: Initiate planning in 1st quarter of FY2000. Start experimentation in 1st quarter of 2001

X. ALP Enabled Alternatives for Transition

What: In the event that ALP is not formally transitioned into a Service-led status, Office of the Secretary of Defense and Joint Chiefs of Staff should prepare an alternative transition path which might be slower and have more steps. The CINCs and TRANSCOM, which are joint entities, will in the end derive substantial support from the commercial sector, whose best practices and operational software are embraced by ALP's architecture structure. Just as in recommendation IX, U.S. Joint Forces Command, with TRANSCOM and DARPA, should plan and conduct a set of experiments to combine existing or soon-to-be available joint products (JTAV and GTN are examples) and world class management and scheduling tools (examples are Warehouse Management Systems and SABRE). The deployment experiments (recommendation IX) should be supported by such information systems. These will be available long before similar Service products. More importantly these are exercised daily by substantial user groups which means that the bugs and errors surface rapidly and are corrected. Many of the existing legacy systems do not have large user groups. The same comment can be made about security.

Who: U.S. Joint Forces Command and TRANSCOM, supported by DARPA, should make their experiment alternative part of the commercially-based deployment experiment.

When: Initiate planning in 1st quarter of FY2000. Start experimentation in 1st quarter of 2001.

XI. Expand the DARPA led Virtual Airline initiative to air freight, sea and land freight.

What: The DARPA-TRANSCOM Virtual Airline shows much promise in stabilizing an effective collaborative environment which could provide DoD with substantial lift and throughput capability possibly beyond what is available with CRAF and VISA.

Who: TRANSCOM should lead the follow-on program with assistance from major Service users.

XII. Structure a Cost-Advantageous Prognostic Program

What: The commercial world has already established the benefits of diagnostics and prognostics. DoD is following in their path with its reader systems. The biggest payoff could be realized in the near term with legacy systems. Experiments to define these and establish the best course of action should be undertaken.

Who: DUSD(L) should use existing coordination mechanisms to establish and execute a series of experiments to find a low cost approach for near term application. If possible it should have a sturdy commercial base of applications and transition.

When: Initiate investigation during 1st quarter of FY 2000. Start experiments within 6 months.

XIII: Improving OCONUS Access Through Interagency Initiatives

What: As was discussed earlier, U.S. public and private resources (as well as those of major allies) are employed by both government-related and private institutions to field infrastructure – such as airports, seaports, roads, water purification. These enhance the operational capabilities of power projection forces. Interagency coordination could lead to a valuable set of improvements which are:

- Infrastructure would be built to standards which accommodate military needs
- Detailed information on planned and as-built infrastructure could enrich databases needed for access planning and execution
- The cost of accomplishing the above is likely to be much less than those of the standard process now employed

Who: The Joint Chief specifically a combination of the J-4 and J-7, should undertake establishing the interagency process and involve the Services, CINCs, and TRANSCOM as appropriate.

When: Initiate in 2000

ANNEX A. ARMY SCIENCE BOARD STRATEGIC MANEUVER EXECUTIVE SUMMARY

THE TASK

General Reimer initiated our study with a simple question "How can we get Army Forces to the fight faster?" By "faster" he meant ensuring the early arrival of critical maneuver units as part of a joint force to meet the needs of the National Military Strategy. His specific requirement to have a composite mounted brigade in 120 hours by sea lift was expanded to include two brigades by air in 96 hours (one Strategic Brigade Airdrop, one Strike Force) and a three division corps with sustainment in 30 days. Naturally we formed a study group! The DCSOPS LTG Burnette, DCSLOG LTG Coburn, CG, AMC General Wilson, and Military Deputy to the ASA (ALT), LTG Kern were appointed as our sponsors. General Shinseki, our new Chief of Staff, confirmed the need for this study with his stated vision for strategic responsiveness: adding more punch to the light forces and lightening the heavy force.

We postulated that Army Forces will operate within a joint and combined theater of operations and would be provided in an approach which we termed strategic maneuver. We defined *Strategic Maneuver* as *"The ability to project military power rapidly from all points of the globe to converge simultaneously with overwhelming land, air, space, and maritime forces which paralyze and dominate the enemy. The objective is to wrest the operational initiative, achieve dominance, and prevent or terminate conflict by defeating the enemy or setting the conditions for sustained decisive operations of follow-on campaign forces if they are necessary."*

This definition required us to assess strategic maneuver holistically, looking at the complete fort-to-fight requirement rather than the more traditional port to port strategic deployability perspective. This caused us to examine all methodologies that enable Army forces to gain strategic maneuver capabilities. We looked at both immediate solutions as well as long-range solutions focused upon the time frame beyond 2010. We were given eight Terms of Reference (TOR) by our sponsors:

1. To identify mobility enablers for early and continuous entry of forces and supplies into and within the theater of operations;
2. To address the implications of an enemy "anti-access" capability;
3. To identify enablers to realize the full potential of the RML pertaining to providing the required sustainment to employ the early deploying force;
4. To review and assess contemplated mobility related experiments, ATDs, and ACTDs;
5. To review and assess current and planned mobility related acquisitions;
6. To identify opportunities for the Army/DOD to leverage commercial capabilities;
7. To assess the current programmed assets to meet identified challenges and shortfalls; and

8. to provide actionable recommendations, which have suitable POM and JROC implementation.

OUR APPROACH

Given these terms of reference and the Chief of Staff, United States Army's (CSA) guidance to "get our forces to the fight faster," our approach centered on four main areas: Command and Control, Mobility, Sustainment, and Analysis. Our unifying concept was to determine what needs to be done to make quicker and better decisions, reduce what needs to be moved, reduce transit time, and reduce sustainment requirements. We worked closely with two other study groups. General Abrams' sponsored Army Science Board focused on future force design of combat systems and LTG Burnette's initiated Strategic Mobility Workshop. We also built upon the Army Science Board Summer Study of 1998, "Concepts and Technologies for the Army beyond 2010," which was led by Dr. Braddock, GEN Gorman and LTG Funk. Our work then builds upon these efforts and focuses on those enablers that maximize the projection of Army forces to get to the fight faster. We must change, with clear evidence, the current perception that our Army takes too long to be effectual.

THREAT/ENVIRONMENT

In our analysis, we did not postulate a specific threat scenario. Rather, we used what was made available through the series of studies, to include the most recent Army After Next war games. We benefited from the AAN Force Projection War Game conducted at Ft. Eustis, VA and the Army After Next War Game conducted at Carlisle, PA. General Maddox, our co-chair, was mentor to this year's game and assisted us to think through the effect of a thinking opponent beginning the fight in our homeland. We did not pose a specific threat, but we did consider impacts to strategic mobility in benign, disrupted, and opposed settings.

A thinking opponent must counter our asymmetric deployment requirements and will begin disruption at our CONUS forts and transportation nodes, not to mention affecting support of the general populace. Perhaps most importantly, cyber disruption, the information warfare starting even before the shooting starts, is critically important and study on this issue is required. A thorough assessment of this threat is required. It can be reasonably assumed that the future threat will seek to strike quickly, then assume a general defensive posture that includes an aggressive anti-access strategy. He will attempt to delay, disrupt, and deny our access to the theater through political, informational and physical means. Asymmetric methods to accomplish this are smart mines at maritime choke points, use of cheap missiles and use of WMD at key transport nodes or disrupting our transportation and deployment systems. It may also include terror attacks in both CONUS and Intermediate Staging Base (ISB) locations. For example, a single container "seeded" with explosives, commanded or timed to explode at a critical staging area or transit point, would cause significant delays in deployment time lines and create perceptions of potential havoc. It would certainly imperil the entire connectivity of strategic maneuver.

We also considered the question of who is in charge of security of the deploying force. Simply put there is no one single person in charge of security, although commanders at all levels are responsible. This too needs to be studied intensively as a priority matter.

WHAT WE LEARNED ABOUT THE FORCE PROJECTION PROCESS

Through all of our data gathering and deliberations, some significant considerations emerged:

An overarching conclusion that solutions to reduce deployment time must consider the entire throughput process. Fixing any one problem may not have the desired outcome if not examined from a systems approach.

Deployment Tools

- Commanders do not have good automated movement planning tools
- Scheduling, monitoring, and rescheduling tools are not timely

Perceptions

- Army currently takes too long to deploy significant lethality

Deployment Requirements

- Reducing logistics consumption reduces the deployment requirement
- Split basing can increase combat power availability but may require organizational redesign

Early Entry Forces

- Immediate fixes are possible to increase lethality
- Increasing lethality increases the airlift requirement

Follow On Forces

- Once ships begin arriving, their capacity outpaces air capacity
- Making forces, which now move by sea, air-deployable will increase the requirement for airlift

Commercial Capabilities

- Commercial lift capacity outpaced military lift capability but economic and technical changes limit its availability
- The Army is not exploiting opportunities to obtain critical features in new commercial craft

Critical Problems To Solve

Through a series of work and research periods we tapped experts from the transportation industry, aircraft and shipbuilding firms, supply chain consultants, other government agencies such as the State Area Readiness Command (STARC), and port authorities. We also tried to take advantage of the most advanced initiatives within DoD to help us get our arms around the totality of this subject. We were able to develop some critical questions as we conducted our research and analysis.

Each of the four panels in this effort is preparing much more detailed reports which deal with the broad range of these critical problem areas.

"Can we make command and control more timely and accurate?" A CINC does not have the automated tools to assist in deployment planning, determining what forces should travel by which means to what locations. Further, the time required by the Time Phased Force Deployment System does not allow us to meet our deployment objectives. A capability is required which allows the CINC to influence the process before the force deployment list is codified. Presently a CINC is required to state his requirements, these requirements are then matched and flowed. Currently, there is no methodology which allows the supported CINC to inter-act with this process other than acceptance and rejection of proposed deployment flow of units over time. The schedule needs to be developed in hours rather than days and be capable of being changed likewise. Commercial capabilities may assist in this process.

We asked who is in charge of the deployment? One answer is CINCTRANS. But essentially he only controls one segment of the process usually termed the strategic deployment. Inherently he receives Army forces through Forces Command through Atlantic Command as the force provider. TRANSCOM then hands the deployment off to the supported CINC. The process is not seamless. This compartmentalization also presents serious security demands in terms of force structure and jurisdiction. We need to look at what must be done to provide real-time information flow to these entities to insure flow management.

None of this activity will take place in an Army-only environment. The joint nature of U.S. military operations must be accepted and facilitated. But to say that the Army merely has to respond to the joint initiatives or requirements is short sighted. As the principal deploying component of the Armed Forces, the Army must play the key and influential role in the development of joint deployment doctrine, tools systems and processes, and policy.

As with the transportation assets of the commercial sector, management and control capabilities have experienced a phenomenal growth in their application and sophistication. Major American and international intermodal companies have made significant investment to ensure that their logistics and transportation functions are a source of ever-increasing productivity. The Army needs to be able to capitalize on this vast resource in as many applications as possible. The DARPA sponsored Advanced Logistics Project (ALP) offers a means to infuse those commercial capabilities into our own planning and management systems and to make our interface with the commercial sector seamless.

"How can we get more capability to the fight earlier?" In order to increase the lethality, survivability, and tactical mobility, work on organizational design must look to improve unit effectiveness, readiness to fight immediately upon entry into the theater, and to do so with less personnel and equipment than at present. This includes a careful look at what functions in our existing structures do not need to be performed in the theater (split base operations), or, in a new method of operating, may not need to be performed at all. With an aggressive set of criteria to examine unit size, functions, capability, and place of operation, we can examine what can be done to bring greater capability earlier in the process.

Equipment design (size, weight, operating characteristics) goes hand in hand with organization design and offers complementary opportunities to build early effectiveness into the theater. Controlled dimensions and weight significantly expand the number of commercial transport assets that can be utilized for deployment. Compatibility with commercial transportation means is key to the use of the very productive and capable global commercial transportation industry.

Reducing the consumption of the deploying force has significant ramifications. The operating characteristics of the equipment such as fuel consumption, probability of kill, and ease of maintenance can make meaningful contributions to deployment enhancement and to follow-on sustainment.

Packaging the unit, whether combat vehicles or supporting equipment and stocks, into modular shipping units further enhances access to the vast assets of the global commercial sector, simplifies the handling at major transfer nodes, and can facilitate the tracking of these units through the entire connectivity of strategic maneuver. Use of such methods and transport assets can also introduce discipline and control into the deployment process from its start point.

The producers of transport assets, the aircraft manufacturers and shipbuilders, are developing aircraft with much greater lift capacity and ships capable of higher speeds than are presently possible. The Army has an interest in these developments, particularly as these improvements might contribute to enhanced deployment. We must work to influence the development of transport platforms. The concept of National Defense Features (those militarily useful capabilities built into a transport asset not required for commercial operation, e.g. special ramps, higher deck strength) can play a key role in the development of such projects as the Fast Ship."

"How do we exploit the growth in capacity in the commercial transportation industry?" Just as the entire commercial world has worked hard at "re-inventing" itself, the transportation industry as a sector has had to work doubly hard. It has had to boost productivity for its own corporate health and has had to boost productivity because the shipper industries have focused on transportation and logistics as their source of improved performance.

The trend in the industry is to greater capacity in the air freight sector which today moves 50,000 tons per day, perhaps as much as fourfold, worldwide, in the next 25 years. If the Army cannot take advantage of this great increase in capacity because its equipment is too large to fit through the doors or too heavy for the cargo deck loadings, we will forego a tremendous capability. If we do not influence future design, we will fail to exploit its great capability. We must interface seamlessly at transfer nodes and must take advantage of the commercial capabilities and efficiencies as far forward as possible. We must focus our organic, special assets at the most challenging operational settings.

In the ocean shipping industry, containerization continues to be the major growth sector. That capacity is being concentrated, however, in mega-ships and in a few "load center" deep water super ports outside CONUS where the emphasis is on huge volume, rapid turn-around, and very tight scheduling. The structure of the industry is being further driven by new economic consortia of largely foreign carriers. Only one major U.S. carrier continues to operate in these markets. There is, however, a substantial fleet of smaller (1000 TEU) ships which could provide access to the world's smaller ports. To stay competitive, ports not destined to become "load centers" are looking at a variety of innovations such as the "Agile Port" and "Rapid Rail" concepts.

American railroads are participating in similar trends. Mergers and acquisitions are producing greater concentration and less system slack. Evolving rail corridors may well leave the Army behind.

In sum, despite massive growth in the industry (now a $500 billion/yr sector), there is little room for Army deployment cargo, especially if it is not immediately compatible with the commercial size and weight constraints and able to integrate seamlessly into a system driven by commercial obligations. If the Army is to construct a seamless interface with the commercial transportation industry, we will have to do it by forming strategic, collaborative partnerships, not through the near-confiscatory CRAF and VISA arrangements.

"How can we improve military lift capability?" While we have stressed the development of military capabilities which can mesh seamlessly with the commercial industry, and we have advocated the reliance on commercial assets, methods, and capabilities as much as possible, there remains the requirement to maintain (or in some cases, develop) unique military capabilities or to insist that military equipment have extraordinary operating characteristics.

Because of the problems of access to the theater, we cannot be dependent solely upon highly developed and sophisticated facilities. We need to be able to use a broad range of airfields and seaports where the operating environment may not support the requirements of advanced international commerce. We also need more reliable data on the broad range of facilities. Many airfields have not been certified for certain aircraft operations. By having more extensive knowledge of these facilities, many more options may exist to enhance our access. Austere airfields, even road segments or open fields, may have to be used. Port facilities without significant materials handling gear, or beaches with inland clearance routes may have to be used. And they may have to be put to use quickly, with a minimum of force structure, and then rapidly closed and relocated. Through all of this, we must maintain the situational awareness of our force, where its pieces are, and what sustainment is required for it.

Consequently, aircraft with austere field capability (C-130, C-17) will need to be focused on these challenging parts of the deployment continuum in order to meet operational goals, to take maximum advantage of their unique capabilities, and to keep the rest of the deployment system operating at peak efficiency on the segments for which they are best suited.

"How can we counter threat actions and options?" Because potential areas of operation may have a limited number of air and sea ports, the capacity of which may further limit force arrival, alternative means must be sought. A thinking and capable enemy will also attempt to target the large, capable fixed facilities in order to limit our access as well.

While not a requirement in every case, the Intermediate Staging Base (ISB) can provide a secure, high throughput facility when circumstances call for it. In most scenarios the ISB is likely to be an essential operating facility. The ISB would be established outside the adversary's targeting range or outside his political sphere of influence. It would take advantage of existing, sophisticated capability, serving as an efficient transfer point from high volume commercial carrier to a range of tactical, intratheater transport means which can serve smaller, austere ports. This would then confront the adversary with an uncertain, wide-ranging access capability of the deploying force.

The use of the ISB is not without a price. Because it is a trans-shipment point, it can add to the time flow and it adds "touches" to the process. It will also require infrastructure (personnel and equipment) to operate. But because it is such a likely option to be invoked, examination of the force structure and operating concepts must be explored.

"Where can we accelerate throughput?" At every point across the deployment/employment continuum, there are opportunities to reduce the amount of handling, administrative actions, and time to process. We refer to these as "touches," be they physical or electronic. There are far too many "touches" in the current system, and there are excellent opportunities to reduce them dramatically. Commercially this is a fertile area of endeavor for increased productivity.

At origin (post, camp or station) equipment can be maintained in a ready-to-load or already loaded for movement status. At Indiantown Gap, PA, we visited the controlled humidity preservation (CHP) warehouses of the Pennsylvania Army National Guard where Abrams tanks and other rolling stock were maintained in mission-ready status. Stored ARNG equipment in CHP warehouses at locations along the littoral make mech force equipment more readily available for loading and will save time.

On the fort-to-port leg improved management and proper integration with the commercial transportation sector are required to ensure that the Army's movement requirements can be accommodated in an increasingly busy and intensively scheduled transport network.

That same requirement carries over to the ports, where the same high productivity pressures have fostered significant investment in sophisticated handling and port management tools. The "Agile Port" and the "Rail Express" project are solid manifestations of this economic necessity.

Speed on the strategic leg en route will also make a great contribution. Development of ocean vessels of significant capacity capable of speeds in excess of 40 knots can make a great contribution to deployment time reductions. Aircraft capable of much larger payloads can do so as well. But if the system is not addressed holistically, we could invest heavily in some aspect of improvement, only to lose that time improvement to poor management or more complicated transfers, thus squandering the value of the investment.

On the ports of debarkation (POD), the same imperatives prevail. We need to reduce the number of "touches," take advantage of technical and management improvements of the commercial transportation industry as far forward as possible, maintain a seamless interface when the hand-off must occur, and adapt this all to a variety of access scenarios from benign to contested.

As the deploying force reaches the "final mile" of this process, as it prepares to conduct its mission, the deployment process and means employed should find that "final mile" to be the logical, seamless, and natural conclusion to the process. Intratheater lift becomes even more critical as we move more and more toward exploiting commercial lift elsewhere.

Because of threat capabilities, political constraints, the physical condition of the infrastructure in the theater, there is a need to cope with multiple and dispersed ports of debarkation, to open and close them quickly and efficiently, and to maintain certain unique capabilities which are not available or required by routine commercial operating practices. Such capabilities as Logistics-over-the-Shore and airfield operating teams are examples.

There are opportunities on every segment of this process, and there are opportunities when the system as a whole is evaluated. It is the optimization of these elements, not just going faster, that will produce the greatest results.

RECOMMENDATIONS

Deployment Command and Control

- Increase Army participation in Advanced Logistics Project (ALP) development
- Place Army personnel in DARPA program office
- Fund Army programs (e.g., GCSS-A, CSSCS) to integrate ALP architecture

- Encourage ACOM, DISA, and DARPA to include ALP system products into the Joint Theater Logistics ACTD with the objective of demonstrating readiness for early fielding

Information Technology

- Direct the Army Battle Command Systems (ABCS) GOSC to create:
  - An Integrated Product Team (IPT) to:
    - Prepare a clear vision of an Integrated Information Infrastructurė (system of systems) based upon commercial standards, procedures and practices
    - Develop an I.I.I. system of systems architecture
    - Promulgate requirements to assure integration of individual programs into the I.I.I. system of systems architecture
- Support effort to achieve a commercially-based, DoD-wide I.I.I.

Reducing Mechanized Brigade Deployment Time

- Have Army staff, with FORSCOM and NGB, develop operational concept for "NG APS" and within 6 months report back with an implementation plan

Leveraging Commercial Sea Lift

- Forward to the Navy revised Army requirements for strategic sea lift to include high speed sea lift
- Enter into a partnership with the Navy and DoT to pursue Title XI support for HSS and Support the immediate incorporation of National Defense Features (NDF) to support military cargo and austere port operations
- Work with DARPA and the Navy to develop technology alternatives to off-load ships rapidly in austere ports and across the shore
- Advocate (Army Executive Agent) DoD-wide packaging standards consistent with best commercial industrial practices and have TRADOC develop and promulgate the associated TTPs to decrease loading time using containers, flat racks and other intermodal devices (equally applicable to air)

Leveraging Commercial Airlift - Today

- MTMC should evaluate commercial airlift compatibility with current early entry equipment
- Explore high-payoff, military-specific enhancements to the commercial fleet, e.g., doors, floors
- Require that all future early entry equipment be commercial air compatible

- Fully use capability of STARC and RC units to expedite deployments from CONUS (equally applicable to sea)
- Contract with global service companies for rapid augmentation of cargo transfer resources at airports of debarkation and intermediate staging bases (ISBs)
- Solicit DARPA/TRANSCOM to extend their "virtual airline" technology to air, sea and rail freight
- Execute several deployment-sustainment exercises using only commercial means to surface problems, explore limitations and train military planners

Intermediate Staging Bases

- Have TRADOC develop a concept for ISB operations and participate in ACOM's "Focused Logistics: Enabling Early Decisive Operations" concept development
- Conduct/participate in experiments (possibly Joint Contingency Force AWE) to determine the minimum force required for efficient ISB operations

Intratheater Military Lift - Today

- Establish a specific intratheater lift requirement
- Use the C-17 as an intratheater lifter into austere airfields when ISBs are activated; practice/train this procedure
- Conduct experiment to determine the minimal efficient force, to include C^2, required to open and operate unimproved airfields and austere sea ports and across the shore
- Development of means to off-load ships rapidly in austere ports addressed in "Leveraging Commercial Sea Lift"
- Increasing Lethality, Survivability, and Tactical Mobility of Early Entry Forces
- Have TRADOC experiment with alternative, available equipment and recommend, within 12 months, needed procurements
- Have TRADOC and XVIII Airborne Corps develop split-based support options, to include necessary organizational redesign
- Work with TRANSCOM to find deployment configurations (packaging) to reduce time
- Develop the justification and approach DoD and Congress for funding in 12 months
- Conduct expeditionary experiment within 24 months (possibly Joint Contingency Force AWE) to examine improvements in early entry deployment and capability

Increasing Lethality, Survivability, and Overall Deployability - Future Forces

- Make the commercial lift sector a true strategic partner
- Request TRANSCOM develop data essential for exploiting the potential of austere airfields and sea ports
- Have DCSOPS and TRADOC establish clear intratheater air requirement and engage CINCs, JCS and Air Force on SSTOL replacement for C-130
- Have TRADOC establish the requirement for Joint Transport Rotorcraft to be able to lift 20 tons and TEU (sea level, 95°F). Army is executive agent. AAE should assure successful acquisition.
- Have requirements for future vehicles (e.g., Multi-Mission Combat System, Future Combat Vehicle, Future Scout Cavalry System) address transportation requirements compatible with the systems' mission
- Have TRADOC examine both traditional platform centric solutions as well as non traditional "ensemble" solutions for future combat systems. Army concept experimentation is needed
- Expand lessons learned from 2nd ACR effort and conduct necessary experiments in split basing, modularity, and containerization for the remainder of the Army

What Can Be Achieved

- Timely and accurate planning, scheduling, and execution tools with full collaboration with commercial lift sector
- Increased lethality, survivability, and tactical mobility for rapidly deployable early entry forces-current and future
- Increased ability to leverage commercial air and sea lift capability
- Improved military lift and transfer capability, particularly in the intratheater role
- Use of ISBs and austere ports to counter threat options and actions
- Improved throughput and logistics, not just increased speed

PART V. GLOSSARY

GLOSSARY

AB	Air base
ABL	Armored Box Launcher
ACC	Architecture Coordination Council
ACTD	Advanced Concept Technology Demonstration
ADCI	Assistant Director of Central Intelligence
AEF	Air Expeditionary Forces
AFCERT	Air Force Computer Emergency Response Team
AFWIC	Air Force Warfare Information Center
AGL	Above Ground Level
AIM	Advanced Information Management
AIP	ASARS Improvement Program
AIWS	Advanced Interdiction Weapons System
ALP	Advanced Logistics Project
AODA	Attack Operations Decision Aid
AOR	Area of Responsibility
APOD	Aerial Port of Debarkation
APOE	Aerial Port of Embarkation
ARPA	Advanced Research Projects Agency
ASD(C^3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ATACMS	Army Tactical Missile System
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
ATR	Automatic Target Recognition
ATSB	Advanced Tactical Support Base
AVLB	Armored Vehicle Launched Bridge
BADD	Battlefield Awareness and Data Dissemination
BAT	Brilliant Antitank
BB	Breakbulk
BDA	Battle Damage Assessment
BPS	Bits Per Second
BW	Biological Weapons
C^2	Command and Control
C^2OTM	C^2 on the move
C^3	Command, Control, and Communications
C^4	Command, Control, Communications, Computing
C^4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CALCM	Conventional Air-Launched Cruise Missile
CC&D	Camouflage, Cover, and Deception

CCC&D	Counter CCAD
CERT	Computer Emergency Response Team
CHP	Controlled Humidity Preservation
CIA	Central Intelligence Agency
CIC	Combined Intelligence Center
CICMP	Community Intelligence Collection Management Program
CINC	Commander-in-Chief
CJCS	Chairman, Joint Chiefs of Staff
CLS	Capsule Launch System
CMOS	Complementary Metal Oxide Semiconductor
CMS	Community Management Staff
CND	Computer Network Defense
COE	Common Operating Environment
COI	Community of Interest
CONUS	Continental United States
COTS	Commercial-off-the-Shelf
CRAFT	Civil Reserve Air Fleet
CS	Combat Support
CSRL	Common Strategic Rotary Launcher
CSS	Combat Service Support
CTP	Common Tactical Picture
DAASC	Defense Automatic Addressing Service Center
DADS	Distributed Agile Deployment and Sustainment
DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DASSL	Demonstration of Advanced Solid State LADAR
DBO	Dynamic Battle Order
DCC	Distributed Combat Cell
DCI	Director of Central Intelligence
DDB	Dynamic Database
DDCI	Deputy Director of Central Intelligence
DDR&E	Director, Defense Research and Engineering
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DLA	Defense Logistics Agency
DMI	Director of Military Intelligence
DMIF	Dynamic Math-Users Information Fusion
DMT	Distributed Mission Training
DoD	Department of Defense
DOE	Department of Energy
DPG	Defense Planning Guidance
DRI	Defense Reform Initiative
DRID	Defense Reform Initiative Directive
DS	Digital Support
DSB	Defense Science Board
DSMAC	Digital-Scene-Matching Area Correlator

DTOG	Debarkation Time on Ground
DTRA	Defense Threat Reduction Agency
DUSD(L)	Deputy Under Secretary of Defense for Logistics
EDI	Electronic Data Interchange
EDRB	Expanded Defense Resources Board
EFP	Explosively Formed Penetrator
ELINT	Electronic Intelligence
EMSEC	Electromagnetic Security
EO	Executive Order
EOC	Extended Operating Conditions
ETOG	Embarkation Time on Ground
EW	Electronic Warfare
FAR	Federal Acquisition Regulators
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEBA	Forward Edge of the Battle Area
FEMA	Federal Emergency Management Agency
FDBS	Fast Deployment Basing Ships
FIA	Future Imagery Architecture
FLIR	Forward-Looking Infrared
FSS	Fast Sealift Ship
FYDP	Future Year Defense Plan
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GEO	Geostationary Earth Orbit
GOTS	Government-Off-The-Shelf
GTN	Global Transportation Network
HE	High Explosives
HEL	High-Energy Laser
HEMTT	Heavy Expanded Mobility Tactical Truck
HET	Heavy Equipment Transporter
HF	High Frequency
HHS	Health and Human Services
HIMARS	High Mobility Artillery Rocket System
HMMWV	High-Mobility, Multipurpose Wheeled Vehicle
HPM	High-Power Microwave
HPSCI	House Permanent Select Committee on Intelligence
HSS	High Speed Sealift
HSMV	High Speed Mobility Vehicle
HUMINT	Human Intelligence
IBS	Intermediate Staging Base
IC	Intelligence Community

IC EXCOM	Intelligence Community Executive Committee
ID	Intrusion Detection
ID	Identification
IDA	Institute for Defense Analyses
III	Integrated Information Infrastructure
IIR	Imaging Infrared
IM	Insensitive Munitions
IMINT	Imagery Intelligence
INFOCON	Information Condition
INR	Bureau of Intelligence & Research
INMARSAT	International Maritime Satellite
INS	Inertial Navigation System
IO	Input, Output
IOC	Initial Operating Capability
IP	Internet Protocol
IPA	Intergovernmental Personnel Act
IPRG	Intelligence Program Review Group
IPS	Illustrative Planning Scenario
IR	Infrared
IPT	Integrated Product Team
ISB	Intermediate Staging Bases
ISP	Internet Service Provider
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITU	International Telecommunications Union
I&W	Indications and Warning
IW	Information Warfare
JASSM	Joint Air-to-Surface Standoff Missile
JBREWS	Joint Biological Remote Early Warning System
JCATS	Joint Conflict and Tactical Simulation
JC^{2}WC	Joint Command and Control Warfare Center
JCS	Joint Chiefs of Staff
JDAM	Joint Direct Attack Munition
JEDMICS	Joint Engineering Data Management Information and Control System
JFACC	Joint Forces Air Component Commander
JFC	Joint Forces Command
JI^3	Joint Integrated Information Internet
JIC	Joint Intelligence Center
JLOTS	Joint Logistics Over-the-Shore
JMIP	Joint Military Intelligence Program
JMIS	Joint Military Information System
JPO-BW	Joint Program Office, Biological Warfare
JROC	Joint Requirements Oversight Council
JROF	Joint Rapid Response Operations Force
JSEAD	Joint Suppression of Enemy Air Defenses

JSEO	Joint System Engineering Organization
JSOW	Joint Standoff Weapon
JTAV	Joint Total Asset Visibility
JT&E	Joint Test and Evaluation
JTF	Joint Task Force
JTF-CND	Joint Task Force for Complete Network Defense
JV 2010	Joint Vision 2010
JWCA	Joint Warfighting Capability Assessment
JWICS	Joint Worldwide Intelligence Communications System
KJ	Kilo Joule
KM	Kilometer
LADAR	Laser Radar
LAN	Local Area Network
LAV	Light Attack Vehicle
LEO	Low Earth Orbit
LID	Light Infantry Division
LLNL	Lawrence Livermore National Laboratory
LOC	Line of Communication
LOCAAS	Low-Cost Autonomous Attack System
LPD	Low Probability of Detection
LMSR	Large Medium-Speed Roll-On/Roll-Off
LSBR	Landing Ship Ballasting Ramps
MALD	Miniature Air-Launched Decoy
MANPAD	Man-Portable Air Defense
MASINT	Measurement and Signature Intelligence
MAV	Micro Air Vehicle
MCCDC	Marine Corps Combat Development Command
MC&G	Mapping, Charting and Geodesy
MEB	Marine Expeditionary Brigade
MECCN	Minimum Essential Command and Control
MEMS	Microelectromechanical Systems
MIT	Massachusetts Institute of Technology
MLRs	Multiple Launch Rocket System
MMCS	Multi-Mission Combat System
MMTD	Miniaturized Munition Technology Demonstration
MMW	Millimeter Wave
MOE	Measures of Effectiveness
MOG	Maximum Aircraft on Ground
MOPP	Mission Oriented Protective Posture
MOUT	Military Operations in Urban Terrain
MPCO	Military Police Company
MPF	Maritime Pre-Positioning Force
MPF-Future	Maritime Pre-Positioning Force Future
MPEG	Moving Pictures Expert Group

MPS	Megabits Per Second
MPSRON	Maritime Prepositioned Ship Squadron
MRD	Motorized Rifle Division
MRR	Motorized Rifle Regiment
MSC	Maritime Target Indication
MSTAR	Moving and Stationary Target Recognition
MTI	Moving Sealift Command
MTMC-TEA	Military Traffic Management Command Transportation Engineering Agency
MTE	Moving Target Exploitation
MTW	Major Theater War

NAI	Named Area of Interest
NCA	National Command Authority
NCTR	Noncooperative Target Recognition
NDF	National Defense Features
NFIB	National Foreign Intelligence Board
NFIP	National Foreign Intelligence Program
NIC	National Intelligence Council
NIH	National Institutes of Health
NIMA	National Imagery and Mapping Agency
NIPC	National Infrastructure Protection Center
NIPRNET	Unclassified Internet Protocol Routing Network
NIST	National Intelligence Support Team
NMJIC	National Military Joint Intelligence Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NTIA	National Telecommunications & Information Administration

OIS	Office of Intelligence Support
ONI	Office of Naval Intelligence
OODA	Observe, Orient, Decide, Act
OOTW	Operations Other Than War
OSD	Office of the Secretary of Defense
OSS	Office of Strategic Services

PAI	Primary Aircraft Inventory
PAX	Passengers
PFIAB	President's Foreign Intelligence Advisory Board
PKI	Public Key Infrastructure
POD	Point of Debarkation
POE	Point of Embarkation
POL	Petroleum, Oils, and Lubricants
POM	Program Objective Memorandum
PSI	Pounds Per Square Inch
PSYOPS	Psychological Operations

R&D	Research & Development
REC	Radio Electronic Combat
RDTE	Research, Development, Testing and Evaluation
REAP	Re-Locatable Entry Air Points
RF	Radio Frequency
RFP	Request for Proposal
RFS	Radio Frequency Spectrum
ROM	Rough Order of Magnitude
RORO	Roll on, Roll off
RSOI	Reception, Staging, and Onward Integration
RSTA	Reconnaissance, Surveillance, and Target Acquisition
RTIP	Radar Technology Improvement Program
SA	Situational Awareness
SAIP	Semi-Automated IMINT Processing
S&T	Science & Technology
SAM	Surface-to-Air Missile
SAR	Synthetic Aperture Radar
SBA	Simulation-Based Acquisition
SBC	Sea-Base Complex
SBS	Small Bomb System
SCADA	Supervisory Control and Data Acquisition
SCI	Sensitive Compartmented Information
SDI	Strategic Defense Initiative
SDIO	Strategic Defense Initiative Organization
SDVs	Skeet Delivery Vehicles
SEAD	Suppression of Enemy Air Defense
SFWs	Sensor-Fused Weapons
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Routing Network
SOTA	State of the Art
SPOD	Sea Port of Debarkation
SPOE	Sea Port of Embarkation
SSCI	Senate Select Committee on Intelligence
SSTOL	Super Short Take-Off and Landing
STAP	Space-Time Adaptive Processing
STE	Stationary Target Exploitation
STON	Short Ton
TAA	Tactical Assembly Area
TACOM	Tank and Automotive Command
TAI	Target Area of Interest
TAPS	Theater Air Planning Segment
TBMCS	Theater Battle Management Core System
TBMD	Theater Ballistic Missile Defense
TCT	Time Critical Targeting

TERCOM	Terrain Contour Matching
TEU	Twenty-Foot Equivalent Unit
TIARA	Tactical Intelligence and Related Activities
TLAM	Tomahawk Land Attack Missile
TLE	Target Location Error
TMD	Tactical Munitions Dispenser
TOA	Time of Arrival
TOE	Table of Equipment
TOG	Time on Ground
TOW	Tube-Launched, Optically Tracked, Wire-Guided Missile
TPED	Tasking, Processing, Exploitation, and Dissemination
TPO	Transformation Program Office
TRADOC	Training and Doctrine Command
TRANSCOM	U.S. Transportation Command
TTP	Tactics, Techniques, and Procedures
TUAV	Tactical UAV
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Air Vehicle
UGS	Unattended Ground Sensors
UHF	Ultra High Frequency
ULF	Ultra Light Force
USACOM	United States Atlantic Command
USAF	United States Air Force
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USN	United States Navy
USSOCOM	United States Special Operations Command
USSR	United States of the Soviet Republic
UTE RATE	Utilization Rate
UXV	Unmanned, Air, Land, Sea or Ground Vehicle
VCJCS	Vice, Chairman, Joint Chiefs of Staff
VHF	Very High Frequency
VLS	Vertical Launch System
VPN	Virtual Private Network
VTOL	Vertical Take-Off and Landing
VSTOL	Vertical Short Take-Off and Landing
WHO	World Health Organization
WMD	Weapons of Mass Destruction
WWW	World Wide Web